1987 – 2007 | Excellence in Access and Privacy
... 20 Years in the Making

INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO
2007 ANNUAL REPORT

Information and Privacy
Commissioner Ontario
Commissaire à l'information
et à la protection de la vie privée Ontario

May 21, 2008

The Honourable Steve Peters
Speaker of the Legislative Assembly

I have the honour to present the 2007 annual report of the Information and Privacy Commissioner of Ontario to the Legislative Assembly.

This report covers the period from January 1, 2007 to December 31, 2007.

Sincerely yours,

Ann Cavoukian, Ph.D.
Commissioner

2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

PERSONALLY, IT HAS BEEN QUITE A JOURNEY FOR ME SINCE THE AUTUMN OF 1987, WHEN I JOINED THE IPC AS THE OFFICE'S FIRST DIRECTOR OF COMPLIANCE. For the past decade, I have had the honour of serving as Commissioner, and during that time, I have seen major changes in both the access and privacy fields – for the latter, primarily arriving from unprecedented advances in technology. For me, 2007 represents a year that will stand out in my mind for the number of positive steps that were taken.

However, it was also a tumultuous year. There are always new challenges, but 2007 brought major advancements for access and privacy. Pivotal orders issued by my office, key court rulings and other developments have raised the bar regarding government transparency and the protection of privacy.

2007 also marked the 20th anniversary of our office first opening its doors in late 1987, as a handful of newly hired staff prepared for the *Freedom of Information and Protection of Privacy Act* coming into effect January 1, 1988. I was lucky to be among the few to join Justice Sidney B. Linden's startup team, in those early days.

Adoption Information Disclosure Act

One of the most significant advances for privacy in Ontario came in September 2007, when Justice Edward Belobaba of the Ontario Superior Court of Justice ruled that sections of the Adoption Information Disclosure Act breached the Canadian Charter of Rights and Freedoms. Most gratifying was the ruling that the privacy-invasive sections of the Act relating to access to birth registration information were "declared invalid and of no force and effect." As the Court noted, the Charter, "... is intended primarily to protect individuals and minorities against the excesses of the majority," and, accordingly, in this case, the charter protected the minority who wished to preserve their privacy.

I had urged the government to amend the proposed legislation to protect the privacy of those involved in past adoptions, giving birth parents and adoptees the right to file a "disclosure veto," which would allow them the option of blocking access to the birth registration information. While this would provide much-needed protection for the minority, it would, also, as the Court noted, "... in fact allow the vast majority to get the information they were seeking."

My first response to the court ruling was one of elation! I immediately thought of all the birth parents and adoptees who had sent me so many heart-wrenching letters, e-mails and

phone calls expressing their concerns – and their fears – at the prospect of having their sealed files opened and the potential impact on their lives. I wrote to everyone for whom we had contact information with the good news.

My feeling of optimism for the future of privacy rights in Ontario grew when I reread the Court's decision.

> People expect, and are entitled to expect, that the government will not share their confidential or personal information without their consent.

It is of critical importance that we never forget the Court's words, "... privacy is undeniably a fundamental value in Canadian society," because privacy is the very underpinning of liberty – the very foundation upon which our freedoms are built.

In November, I publicly applauded Premier Dalton McGuinty for his decision not to appeal the Court ruling and was extremely grateful for his decision. I also pledged the full support of my office in drafting a new law that would include a disclosure veto, allowing the individuals involved in past adoptions the option of exercising their right to privacy. After my office worked with the government, the resulting bill was introduced in the Legislature on December 10, with the government aiming at having the new law in place by the spring of 2008.

Used-Goods Decisions

Two other very positive steps for privacy in Ontario revolved around the same core issue – that the collection of extensive personal information from individuals whose only wish was to sell one or more second-hand items to a used-goods store, should not end up in police files. The first development was a court ruling; the second was a seminal order that I issued.

In July, the Ontario Court of Appeal struck down a City of Oshawa bylaw that had required used-goods retailers to collect extensive personal information from people who wanted to sell one or more second-hand items to such stores. This personal information, comprised of a photograph and the particulars of three pieces of government-issued identification, was then to be transmitted to, and stored centrally in, a police database, without any restrictions on its use or any judicial oversight.

In September, for the first time in the 20-year history of my office, I invoked the power to order an institution to cease the collection of personal information. In Order MO-2225, I directed the City of Ottawa and the Ottawa Police to stop collecting extensive personal information from individuals selling used goods to second-hand stores and to destroy all personal information already collected (with limited exceptions).

We then published a set of guidelines – *Privacy Guidelines for Municipalities Regulating Businesses Dealing in Second-hand Goods* – in an effort to provide assistance to all municipalities and police services throughout Ontario. (For more information on MO-2225, see the *High Profile Privacy Incidents* chapter.)

Privacy Laws Not at Fault

There is, of course, no shortage of new challenges in access and privacy, and in 2007 I found myself in the unique position of having to defend privacy, not only from those who wish to erode it, but from those who seek to employ it as an excuse

or a scapegoat – and for reasons that have nothing to do with privacy, thereby trivializing it in the process.

A spate of newspaper columns, editorials and stories – citing several different incidents – decried privacy laws as "an obstruction to public safety," with public officials blaming privacy laws for everything from allowing an escaped convict to roam about freely, to the tragedy of the Virginia Tech campus shootings. Throughout the autumn of 2007, I found myself writing to four major daily newspapers, ranging from the *National Post* to the *Washington Post*, discrediting the argument that privacy laws jeopardized public safety. The problem cited in each of those incidents was not with our privacy laws, but rather with those who failed to exercise their ability to disclose much-needed information, when required. (See the chapter in this Annual Report entitled, *Don't Hide Behind Privacy Laws.*)

If You Use Public Funds, the Public has a Right to Know

There were a number of other court rulings in 2007 addressing important access and privacy issues. Among these was a very significant ruling by Ontario's Divisional Court in which it upheld two decisions made by my office on the application of the solicitor-client exemption to legal fees.

The July ruling was a strong endorsement of our approach to the disclosure of legal fee information under the *Freedom of Information and Protection of Privacy Act* and its municipal counterpart. The ruling underscores our consistent message that governments should actively disclose information about the expenditure of public funds.

One of the cases involved the amount of legal fees incurred by two ministries in defending lawsuits regarding the province's provision of services to children with autism.

When my office ordered the disclosure of the total dollar amount for the legal services rendered, the government challenged this decision in Divisional Court. This court challenge was heard together with a similar case in which our office had ordered the disclosure of the total dollar amount on invoices for legal services rendered to a ministry in respect of an appeal to the province's Health Services Appeal and Review Board.

The Court agreed with my office's conclusion that no privileged communications would be revealed by the disclosure of the bottom line or total amounts of invoices for legal fees in each of these cases. This was an especially gratifying ruling.

Public Interest Override

In May, the Court of Appeal issued a very significant decision involving an appeal by the Criminal Lawyers Association.

The Court granted the appeal, significantly expanding the circumstances upon which the "public interest override" provision in the provincial and municipal *Freedom of Information and Protection Acts* could be invoked.

For more information on this decision and other key court rulings, see the *Judicial Reviews* chapter in this annual report.

Impact of Technology on Privacy

My office produced a number of key policy papers and fact sheets in 2007 on the impact that technology has – or may have – on privacy. These ranged from *Biometric Encryption:*

A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy, to *Wireless Communication Technologies: Safeguarding Privacy & Security*.

I have devoted a chapter – *Advancing Privacy through Technology* – in this Annual Report to exploring the potential privacy implications of several leading emerging technologies and the related work my office is doing.

Honoured to be Linked with Distinguished Canadian Women

In November 2007, I was honoured to be recognized as one of Canada's top 100 most powerful women in the "Trailblazers and Trendsetters" category for my work in protecting privacy. I feel privileged to share such a distinction with the noteworthy Canadian women who were given this award and I commend the Women's Executive Network for its ongoing work in drawing attention to the outstanding accomplishments of Canadian women in so many walks of life.

My Personal Thanks

I would like to give a very sincere thank-you to all of our IPC staff – past and present. So much has transpired since this office first opened its doors in 1987. Over the years, I have seen the demands and pressures on my office grow significantly and my staff have repeatedly met and exceeded the growing expectations placed upon them. There have been many occasions where I was genuinely touched by the diligence and enthusiasm shown by my staff. I truly believe that the people of Ontario are very fortunate to have such talented and dedicated people working on their behalf, in the pursuit of open, transparent government, and the protection of our personal privacy...essentially, for our freedom and liberty. You are all true professionals. My heartfelt thanks to you all, now as always!

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner of Ontario

TABLE OF CONTENTS

The Purposes of the *Acts*

The purposes of the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act* are:

a) To provide a right of access to information under the control of government organizations in accordance with the following principles:

- information should be available to the public;
- exemptions to the right of access should be limited and specific;
- decisions on the disclosure of government information may be reviewed by the Information and Privacy Commissioner.

b) To protect personal information held by government organizations and to provide individuals with a right of access to their own personal information.

The purposes of the *Personal Health Information Protection Act* are:

To protect the confidentiality of personal health information in the custody or control of health information custodians and to provide individuals with a right of access to their own personal health information and the right to seek correction of such information, with limited exceptions.

Role and Mandate

Ontario's *Freedom of Information and Protection of Privacy Act (FIPPA)*, which came into effect on January 1, 1988, establishes an Information and Privacy Commissioner (IPC) as an officer of the Legislature. The Commissioner is appointed by and reports to the Legislative Assembly of Ontario and is independent of the government of the day.

The term "freedom of information" refers to public access to general records relating to the activities of government, ranging from administration and operations to legislation and policy. It is an important aspect of open and accountable government. Privacy protection is the other side of that equation, and refers to the safeguarding of personal information held by government.

FIPPA applies to all provincial ministries and most provincial agencies, boards and commissions, as well as to universities and colleges of applied arts and technology. The *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*, which came into effect January 1, 1991, broadened the number of public institutions covered by Ontario's freedom of information and privacy legislation. It covers local government organizations, such as municipalities, police, library, health and school boards, and transit commissions.

The *Personal Health Information Protection Act, 2004 (PHIPA)*, came into force on November 1, 2004, and governs the collection, use and disclosure of personal health information within the health-care system. It is the third of the three provincial laws that the IPC oversees.

Together, these three *Acts* establish rules about how government organizations and health information custodians may collect, use, and disclose personal data. They also establish a right of access that enables individuals to request their own personal information and have it corrected if necessary.

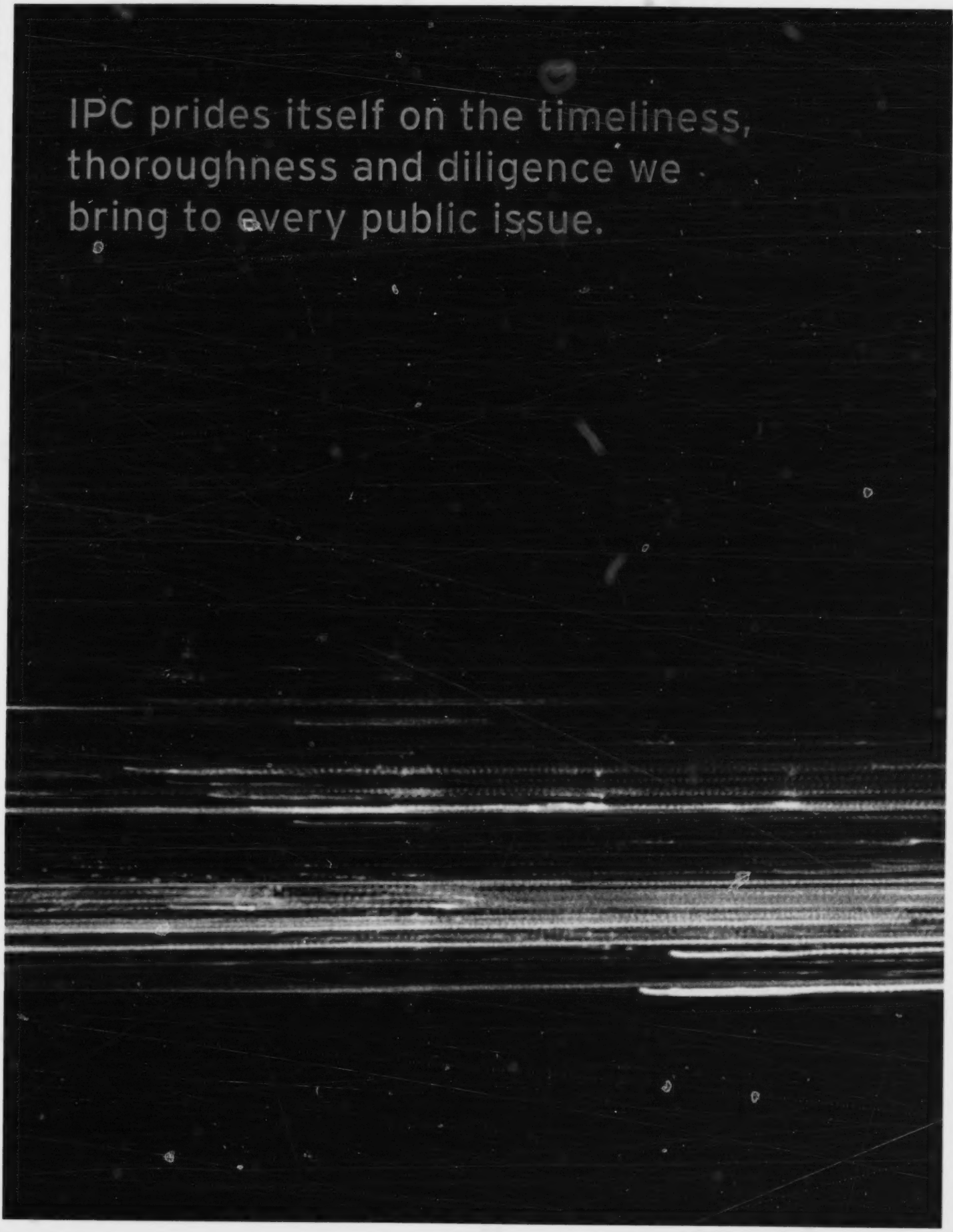
The Commissioner plays a crucial role under each of the three *Acts*. In general terms, the Commissioner's mandate is to:

- independently review the decisions and practices of government organizations concerning access and privacy;
- independently review the decisions and practices of health information custodians in regard to personal health information;
- conduct research on access and privacy issues;
- provide comment and advice on proposed government legislation and programs;
- review the personal health information policies and practices of certain entities under *PHIPA*; and
- help educate the public about Ontario's access, privacy and personal health information laws and related issues.

The Commissioner delivers on this mandate by fulfilling seven key roles:

- resolving appeals when government organizations refuse to grant access to information;
- investigating privacy complaints related to government-held information;
- ensuring that government organizations comply with the *Acts*;
- conducting research on access and privacy issues and providing advice on proposed government legislation and programs;
- educating the public about Ontario's access, privacy and personal health information laws and access and privacy issues;
- investigating complaints related to personal health information; and
- reviewing policies and procedures, and ensuring compliance with *PHIPA*.

In accordance with the *Acts*, the Commissioner has delegated some decision-making powers to her staff. Thus, the Assistant Commissioner (Privacy), Assistant Commissioner (Access) and other designated staff may issue orders, resolve appeals, and investigate privacy complaints.


IPC prides itself on the timeliness,
thoroughness and diligence we
bring to every public issue.

KEY CHALLENGES

Don't Hide Behind Privacy Laws

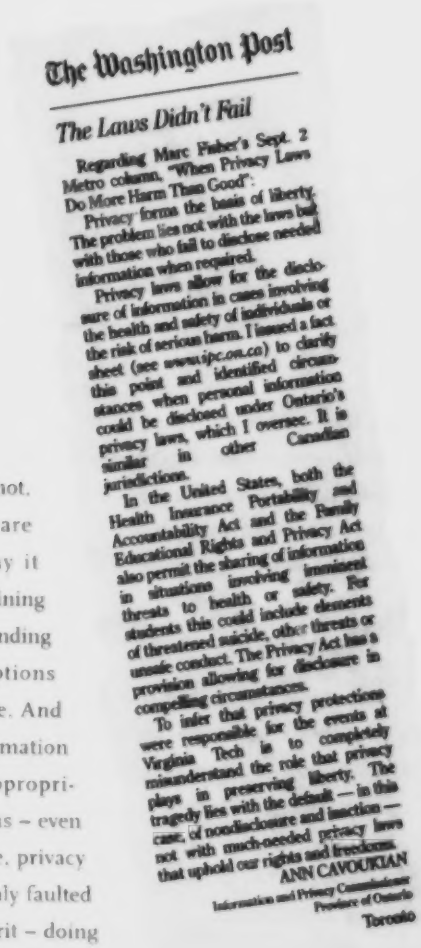
By Ann Cavoukian, Ph.D.
Information and Privacy Commissioner of Ontario

OVER THE PAST YEAR, I HAVE BEEN TROUBLED BY WHAT SEEMS TO BE AN INCREASING TENDENCY FOR PUBLIC OFFICIALS TO HIDE BEHIND PRIVACY LAWS WHEN THE ISSUES AT HAND HAVE IN FACT, LITTLE TO DO WITH PRIVACY.

The public debate surrounding the tragic shootings at Virginia Tech late in 2007 provides an excellent example of this tendency at work. In the aftermath of the tragedy, a key issue that emerged was communication, and how university officials had failed to communicate both with each other and with the parents of the killer prior to the massacre. Officials attributed this failure to their interpretation of the privacy laws they felt bound by; they believed that those laws prohibited them from sharing much-needed information.

Newspapers, perhaps not surprisingly, seized upon this point and sensationalized it. Media reports of the incident were full of claims that privacy laws had prevented university and health officials from disclosing information that could have identified the threat posed by the shooter, thereby preventing the tragedy.

This view is mistaken. As I noted in my letter to the *Washington Post* at the time, the issue lies not with our privacy laws themselves but rather with officials who fail to disclose information when required. Even the panel that reviewed the circumstances surrounding the tragedy noted in its report that the incorrect interpretation of privacy laws "... may cause holders of such information to default to the non-disclosure option – even when laws permit the option to disclose."



The Washington Post

The Laws Didn't Fail

Regarding Marc Fisher's Sept. 2 Metro column, "When Privacy Laws Do More Harm Than Good":

Privacy forms the basis of liberty. The problem lies not with the laws but with those who fail to disclose needed information when required.

Privacy laws allow for the disclosure of information in cases involving the health and safety of individuals or the risk of serious harm. I issued a fact sheet (see www.ipc.on.ca) to clarify this point and identified circumstances when personal information could be disclosed under Ontario's privacy laws, which I oversee. It is similar in other Canadian jurisdictions.

In the United States, both the Health Insurance Portability and Accountability Act and the Family Educational Rights and Privacy Act also permit the sharing of information in situations involving imminent threats to health or safety. For students this could include elements of threatened suicide, other threats or unsafe conduct. The Privacy Act has a provision allowing for disclosure in compelling circumstances.

To infer that privacy protections were responsible for the events at Virginia Tech is to completely misunderstand the role that privacy plays in preserving liberty. The tragedy lies with the default — in this case, of nondisclosure and inaction — not with much-needed privacy laws that uphold our rights and freedoms.

ANN CAVOUKIAN
Information and Privacy Commissioner
Province of Ontario
Toronto

More often than not, public officials are choosing to play it safe instead of gaining a proper understanding of what their options are for disclosure. And then, when information is withheld inappropriately and problems – even tragedies – ensue, privacy laws are mistakenly faulted as being the culprit – doing "more harm than good."

In reality, privacy laws are an essential part of the social fabric of our democracy. Privacy is a fundamental right that helps us to realize the other fundamentals that we value so dearly, like liberty and freedom. And when privacy is falsely pitted against security or public safety, or used as a convenient scapegoat for inaction, it is our very liberty that is threatened. And our attention is drawn away from the real issues at hand: bureaucratic inertia, misguided policies, inefficient practices, and poor judgment.

The problem in the case of the Virginia Tech massacre was not that privacy laws existed – it was that they were misinterpreted and poorly understood by those responsible for implementing them.

It is certainly true that the primary purpose of privacy laws is to protect personal information collected, used or disclosed by public and private sector organizations. But clear exceptions always exist to enable authorities to collect and disclose certain information for specific purposes, such as law enforcement. Privacy laws give government agencies wide latitude when it comes to protecting public safety. It is up to those agencies to exercise that authority appropriately.

In July 2005, I issued a fact sheet entitled, *Disclosure of Information Permitted in Emergency or other Urgent Circumstances* (see www.ipc.on.ca), to clarify this point and identify circumstances when personal information could be disclosed under Ontario's privacy laws. The exemptions include permitting disclosure:

- Where compelling circumstances affecting the health and safety of an individual exist;
- In compassionate circumstances to facilitate contact with a close relative or friend if an individual is injured, ill or deceased;
- In situations where there is a grave health, safety or environmental hazard to the public; or
- Where it is necessary to eliminate or reduce a significant risk of harm to an individual or group.

NATIONAL POST

Don't let public officials hide behind 'privacy'

Re: Officials Cite 'Privacy' In Not Discussing Case, Sept. 14.

I'm getting sick and tired of public officials refusing to release information to the public because of "privacy." When a spokesman for the Canada Border Services Agency was asked for information about a war crimes suspect, she said she couldn't talk about the case. Why? Because of "privacy." Nonsense! There may well be good reasons for not divulging information related to the case, having to do with law enforcement, solicitor-client privilege or court proceedings. But don't blame privacy, which appears to have become the scapegoat of choice.

I'm extending a challenge to everyone in the media: The next time someone tells you they can't tell you something because of "privacy," dig deeper and ask them why. Nine times out of 10, it will probably have nothing to do with privacy and everything to do with avoiding transparency. Make them justify what they tell you.

Ann Cavoukian
Information and Privacy Commissioner/Ontario, Toronto.

The rules are similar in other Canadian jurisdictions.

In the United States, both the Health Insurance Portability and Accountability Act and the Family Educational Rights and Privacy Act permit the sharing of information in emergency situations involving imminent, specific threats to health or safety. The Privacy Act of 1974 has a similar provision allowing disclosure in compelling circumstances.

To imply that privacy laws – rather than the judgment shown in the application of those laws – are to blame for what happened at Virginia Tech is, in my view, irresponsible. A clear understanding of the facts is the essential foundation of our path of action, our social contract, and the choices that policy-makers make on our behalf. Misrepresenting the facts about privacy laws may titillate readers or fire controversy that helps sell more newspapers. But ultimately it focuses public attention, and the attention of our politicians, away from the real issue at hand, which is that laws must be thoughtfully, carefully, and intelligently applied. Especially where public safety is concerned.

When we hear officials citing privacy as a barrier to the public interest, or the media arguing that privacy laws jeopardize public safety, we must learn to demand that these positions be justified. That's why late last year, in a letter to the *National Post*, I challenged the media this way: "The next time someone tells you they can't tell you something because of 'privacy,' dig deeper and ask them why."

Now, I am challenging everyone who is ever told that information could not be released because of privacy legislation to ask:

- Where in the law (section) does it state that the release of the information is specifically forbidden?
- Why (specific reasons) does the law forbid the release of the information?
- When is the release of such information allowable under the law?
- Are there not exemptions with regards to public safety?

I believe that if we begin to ask these questions, and to demand answers, we will see that privacy is not the barrier that some public officials and media outlets would have us believe, but rather a convenient cover for human error, lack of judgment, or inaction.

Privacy is too important to our social fabric to let it come under attack on the basis of false accusations. And I urge all of you – from individual citizens to large corporations to national and international media outlets – to take seriously our responsibility to protect that precious freedom.

WHO ARE YOU? PROVE IT! NEVER BEFORE IN HISTORY HAVE WE BEEN ASKED TO IDENTIFY OURSELVES AS WIDELY, AS OFTEN, OR AS STRONGLY, AS TODAY. NEW INFORMATION TECHNOLOGIES ARE RECORDING OUR DIGITAL IDENTITY DATA, HELPING TO SECURE ACCESS TO SENSITIVE SPACES AND RESOURCES - BUT AT WHAT COST TO OUR PRIVACY?

Advancing Privacy through Technology

INFORMATION – ESPECIALLY PERSONAL INFORMATION – IS A CORE COMMODITY IN OUR DIGITAL ERA. GROWTH AND SUCCESS IN THE DIGITAL AGE DEPENDS, IN PART, ON THE EXTENT TO WHICH THE PUBLIC TRUSTS HOW PERSONAL INFORMATION IS COLLECTED, USED, DISCLOSED AND RETAINED BY THE ORGANIZATIONS THAT HOLD IT.

There is a profound need for these organizations to manage personal information credibly. This requires not only adherence to fair information practices, but also intelligent technology choices.

The IPC has long advocated for the development and deployment of technologies that support privacy aims while delivering on core business objectives. In 2007, we continued our efforts with particular emphasis on promoting privacy-enhancing technologies.

Privacy by Design

Integrating privacy fundamentals into information systems not only enhances privacy, but also data security. Some of these fundamentals include:

- Minimize personal information sought, collected, used, retained and disclosed – if you don't possess the data, you can't lose or misuse it;
- Empower individuals to participate in managing their own personal information – trust depends on openness, transparency and accountability;
- Ensure strong safeguards – include strong audit and compliance measures.

"Privacy by design" begins early, at the conceptual stages of new, large, or complex information systems that process personal information.

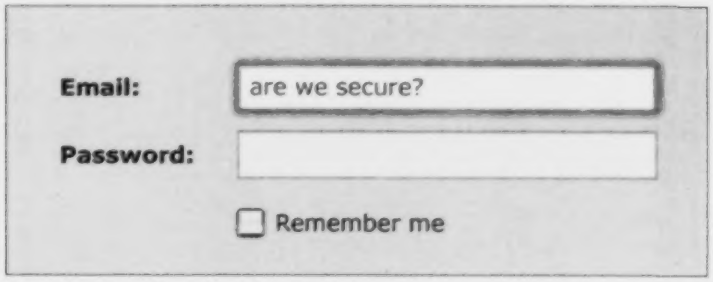
The IPC offers a wealth of guidance materials for effective privacy design, such as privacy impact assessment tools, available online at www.ipc.on.ca.

Secure Technologies

Many privacy risks may be mitigated by deploying widely available technologies, such as encryption. Encryption and other types of signal-scrambling techniques transform data into a format unintelligible to those not in possession of the special passkey to decrypt the information. As long as the passkey is kept secure, the encrypted data cannot be viewed in "plain text" format, even if it is intercepted.

Encryption has a number of other interesting properties that make it suitable for other uses and applications such as secure communications; strong identification, authentication and access control; privacy-enhanced data matching; and data integrity checking.

In 2007, the IPC issued two important health orders in response to data security and privacy breaches, as well as guidance notes on encryption and how to secure mobile devices and wireless video.



Always Think Before You Click: Beware of trading the security of your personal information for convenience.

Privacy-Enhancing Technologies (PETs)

This year, as in the past, the IPC continued to encourage the development and use of privacy-enhancing technologies wherever possible.

PETs incorporate essential privacy fundamentals, or fair information practices (FIPs), directly into the information technology and its operation. They have been defined as "a coherent system of ICT (Information and Communications Technology) measures that protect privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system."

Awareness of, interest in, and demand for PETs appear to be growing around the world. European Commission officials, data protection authorities, standards developers and technology researchers are actively funding and promoting research, development, and implementation of PETs.

The IPC continues to be active in promoting privacy-enhancing tools and technologies. The IPC has engaged companies such as Facebook, Google, IBM, Microsoft, Oracle and others on matters of privacy and security, arguing for improved privacy-enhancing design and functionality options for users.

IPC PETs Research and Development Initiatives

Each year, the IPC presents an award for outstanding research in Privacy-Enhancing Technologies at the PET Workshop (now called the PET Symposium). An independent, international peer-review panel selects the winning papers from among the hundreds submitted.

In 2007, the IPC presented the PET Award to the authors of a paper demonstrating the security risks of RFID-embedded payment fobs.

The IPC also joined with the University of Toronto to launch a new interdisciplinary graduate program combining Applied Science and Engineering with Information Studies. The Identity, Privacy and Security Initiative (IPSI) program supports new approaches to security that maintain the privacy, freedom and safety of the individual, as well as the broader community.

Commissioner Cavoukian chairs the IPSI Advisory Board. She gave the inaugural lecture in September 2007, about how privacy and security technologies should not be viewed as trade-offs in a zero-sum game. Instead, she argued for a positive-sum paradigm, integrating both security and privacy requirements into new information technologies to deliver optimal "win-win" results.

This year, the IPC also concluded fours year of participation in the University of Ottawa's *On the Identity Trail* research project, led by Professor Ian Kerr. The project brought together a multi-disciplinary research team to identify and address failures in bringing privacy-enhancing technologies to market and develop "applications for privacy-enhancing technologies that can find markets in the new economy."

Promoting Use of PETs in Government and Businesses Operations

In 2007, the IPC worked with many public sector and health organizations across Ontario on the direction, shape and

governance of large-scale IT projects that process personal information.

The privacy advice the IPC offered helped support critical architecture, design, and technology choices, as well as governance policies and operational procedures. Some key projects included:

- Health data repositories, entities and registries;
- Interoperable electronic medical records (EMR) systems;
- Public sector interactive Web portals;
- Identity management systems;
- Public video surveillance camera networks;
- Integrated public transit fare cards;
- Contactless smart card applications; and
- Law enforcement information-sharing initiatives.

The IPC also provided advice through a wide range of other avenues, including:

- The Government of Ontario select Independent Advisory Committee, created in 2005 to provide independent expert advice on implementation issues associated with large business transformation initiatives involving ICTs;
- The Ponemon Institute's Responsible Information Management (RIM) Council, Privacy-Enabling Technology Working Group;
- Carnegie Mellon University's CyLab Privacy Interest Group (CPIG);
- The European Biometrics Forum's International Biometric Advisory Council (IBAC); and
- The OECD Workshop on Digital Identity Management.

The IPC also submitted written comments on initiatives in Ontario, Canada, the United States, Europe, and elsewhere on technology and privacy-related issues.

In September, the IPC co-sponsored an international resolution by Privacy and Data Protection Commissioners on developing privacy-related standards for the use and deployment of new and existing technologies.

Biometric Encryption (BE)

Biometrics are unique physiological characteristics, such as fingerprints or iris scans, that can be used to recognize and verify identity. Biometric technologies promise to enhance the effectiveness of identification and authentication processes, help control access to physical and electronic resources, and improve the security of information systems.

Implemented poorly, however, biometric technologies can be highly privacy invasive. Biometric data, once collected, may be stored, shared and used for numerous unauthorized secondary purposes, potentially opening the door to discrimination and identity theft.

While widespread adoption of biometric technologies is on the horizon, the IPC believes that ubiquitous use should not come at the cost of personal privacy. In March 2007, the IPC co-authored a research paper with international biometrics expert Dr. Alex Stoianov, entitled *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy*. The paper illustrates how biometrics may be deployed in a privacy-enhancing manner that minimizes the potential for surveillance, maximizes individual control, and ensures full functionality and enhanced security of the systems involved.

With biometric encryption, instead of storing, for example, fingerprint templates in a database, the live fingerprints are used to encode some other information, like a password or account identifier, or cryptographic key. Only the biometrically encrypted result, not the biometric itself, is actually stored. This removes the need for organizations to collect and store actual biometric images in their database. In this way, many privacy and security concerns associated with the creation and maintenance of centralized databases are eliminated.

Another significant privacy advantage of using BE technology is the ability to generate multiple different outputs (or identifiers) from the same biometric, and to even revoke and create new identifiers, if the need arises – much like changing a password or credit card number.

As an added bonus, BE can enable people to quickly, easily and securely encrypt (and decrypt) their own data, using only their biometric.

With data minimization, user control, and enhanced security, BE qualifies as a true PET. These and many other advantages of BE over traditional biometrics are outlined in our paper, which is available on the IPC's website.

Interest in, and response to, the BE paper – from public policy-makers, industry associations, and biometrics researchers around the world – has been tremendous. We were delighted to learn that a number of publicly funded research initiatives and small-scale trials of BE technology are already underway. Two particularly noteworthy initiatives are:

Private Speaker Identification: Netherlands-based Philips successfully integrated its PrivIDTM "private template" solution with voice biometric technology, creating a world-class, privacy-protected speaker verification solution, with enormous potential for use in remote client or account access scenarios, such as telephone banking.

Private Face Recognition: The Ontario Lottery and Gaming Corporation is exploring the use of facial biometrics to assist Ontarians who voluntarily choose to opt into the self-exclusion program so that they can be denied entry into casinos (because of a self-identified gambling addiction). Because of sensitivities surrounding any use of automatic identification technologies in casinos, a privacy-enhanced solution is essential. In 2007, researchers at the University of Toronto Faculty of Engineering undertook research to develop a "made-in-Ontario" BE solution that may be integrated with facial recognition technology.

Radio Frequency Identification (RFID)

In 2006, the IPC developed and released *Privacy Guidelines for RFID Information Systems* and *Practical Tips for Implementing RFID Privacy Guidelines*. In 2007, the IPC partnered with Hewlett-Packard Canada to research and develop a guidance paper reviewing the many uses and benefits of RFID technology for health-care providers, and providing guidance on how to identify and mitigate the privacy risks. *RFID and Privacy: Guidance for Health-Care Providers* was released in January 2008.

Data Breaches

Even with the application of fair information practices and the use of privacy-enhancing technologies, data breaches will occur. The *Personal Health Information Protection Act (PHIPA)* makes Ontario the only jurisdiction in Canada where notifying patients of privacy breaches is mandatory.

Of the hundreds of breaches reported to the IPC since *PHIPA* came into effect in late 2004, the majority have been relatively small scale and episodic in nature. These include occurrences

Whether visible or hidden, RFID tags wirelessly transmit unique identifiers automatically and silently to any device that asks.

like a lost appointment book or a misdirected fax or letter. Others have been more significant, exposing systemic risks. These have included, for example, incidents of lost laptops containing unencrypted patient information.

Sadly, 2007 was another banner year for reported data breaches. Whether the result of hackers or employees, of malice, neglect or simple error, such breaches undermine public confidence.

Because data breaches can have such a major impact on innocent lives – including putting them at risk for identity fraud and theft – many jurisdictions around the world are adopting mandatory breach notification. This trend towards transparency is a very welcome development.

In 2007, the IPC continued to advocate for greater openness, transparency and accountability for data privacy and security breaches, calling upon the Ontario government to bring in legislation to address breach notification more widely.

The IPC also developed and released a *Breach Notification Assessment Tool*, which is available online at www.ipc.on.ca, as are all IPC papers cited in this Annual Report.

Going Forward

2007 was a busy and productive year for the IPC in terms of promoting PETs and building better understanding of how privacy and technology can interact to the benefit of both.

In an age characterized by revolutionary IT developments and exponential information creation, storage, transmission and use, the case for robust and credible information management has never been greater. It is clear that the time has come for widespread use of PETs and acceptance of the concept of building privacy into the design of emerging technologies. With care, advances in technology will also mean advances in privacy.

In 2008, we will continue our important work in this area, advocating for privacy-friendly technology options for identity management systems, interoperable electronic health records, e-government portals, and many other large public and private-sector IT projects.

Commissioner's Recommendations

1. Make a Privacy-Protective Electronic Health Record a Priority

Ontario needs to move quickly towards implementing an effective interoperable electronic health record (EHR) that may be shared with patients and practitioners across the health-care sector.

This is an essential step for all Ontarians, yet Ontario lags behind other provinces. Development of an EHR is a very important issue that should become a top priority. When health-care professionals can electronically access a patient's complete health record, it will not only save lives, but will drive down costs.

As well as major health-care advantages, electronic health records present some privacy challenges. These challenges, however, can be met with enhanced privacy-protective features ranging from anonymization to user authentication; from strict access controls to electronic audit logs. I am highly motivated to work with the Ontario government to expedite the development and implementation of effective, privacy-protective EHRs in Ontario.

2. Advance the Development of Transformative Technologies

I am calling upon the Premier, who served for years as the head of the Ministry of Research and Innovation, and John Wilkinson, the Minister of Research and Innovation, to advance the development of transformative technologies (privacy-enhancing technologies applied to technologies of surveillance), not only in the area of research, but particularly in the commercialization of such research to facilitate its entry into the marketplace. I would be delighted to offer my assistance to the Premier and Minister, in whatever capacity they feel necessary.

3. Give Families the Information they need after the Death of a Loved One

In an earlier Annual Report and in subsequent public comments, I advocated for an amendment to the provincial and municipal *Freedom of Information and Protection of Privacy Acts* that would enable relatives of deceased persons to obtain information regarding the circumstances of the death of family members. This was based on our experience that local police services and the Ontario Provincial Police were required to deny relatives access to this type of information because disclosure was presumed to be an unjustified invasion of the deceased's personal privacy.

To its credit, the Ontario government subsequently acted and introduced Bill 190, which contained amendments to the *Acts* that would permit institutions to disclose the personal information of a deceased individual to family members in compassionate circumstances.

Despite the fact that Bill 190 passed, our experience to date indicates that some police services are still reluctant to provide greater disclosure to family members. In fact, the existence of the new section permitting the disclosure of the personal information of a deceased individual is often ignored.

In 2007, my office issued its first orders interpreting this new section after individuals appealed the denial of access to the information they were seeking about the death of a family member. These orders recognized that the amendments resulting from Bill 190 were designed to increase disclosure to relatives in order to assist them in understanding the circumstances of their loved one's death, and to assist in bringing some measure of closure to a difficult experience.

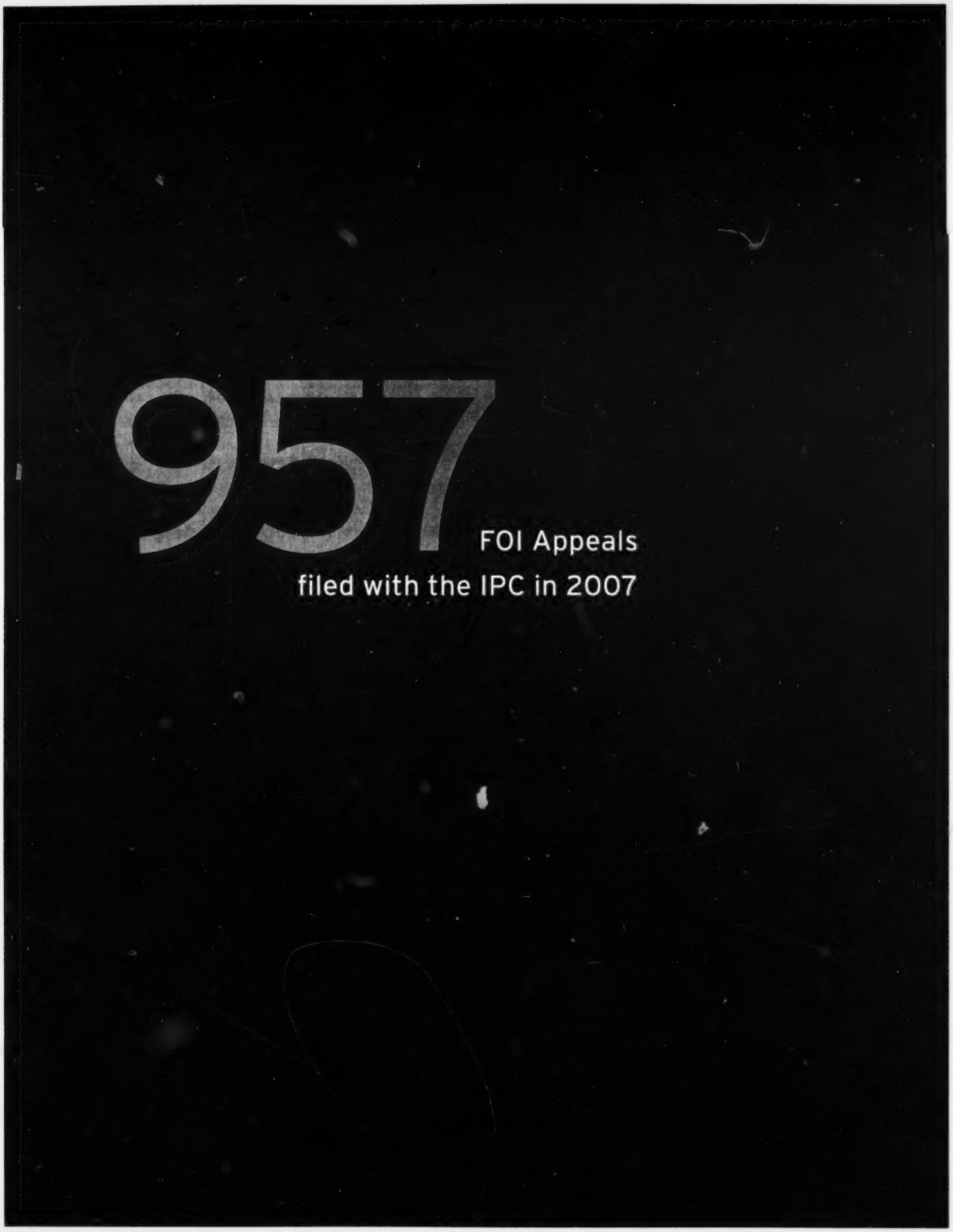
All police services are asked to recognize the intent of the Legislature by giving a broad and generous interpretation to these new sections so that family members may gain greater knowledge of the circumstances surrounding the deaths of loved ones.

4. Make Citizenship Information Available to the Provinces

A number of provinces, including Ontario, are looking at providing an enhanced drivers' licence (EDL) that citizens could use as an alternative to a passport, to cross the U.S. border. Privacy Commissioners from across Canada, earlier this year, issued a joint memorandum calling on all governments involved in such a project to take specific steps to protect privacy. While we supported the joint memorandum, Ontario, after extensive consultations with my office, had already committed to many of the key steps that all governments are being urged to take before implementing an enhanced drivers' licence initiative.

There is, however, an essential step that the federal government must first take. Provinces and territories cannot be required to build their own databases of citizenship information – which is essential for EDLs. To do so would needlessly add to privacy and security concerns, not to mention the costs of a cumbersome and highly duplicative process. Wasting taxpayer dollars, duplicating efforts and creating a mirror database that would serve as a magnet for identity thieves – that would be the result of this federal requirement.

I am urging the Government of Canada to securely provide citizenship information, upon request, to any province or territory that is implementing an EDL program, and abandon the privacy-invasive requirement that provinces recreate this information from scratch.


957
FOI Appeals
filed with the IPC in 2007

Key moments in the evolution of FOI and Privacy in Ontario

WHILE 2007 MARKED THE 20TH ANNIVERSARY OF THE PASSING OF ONTARIO'S FIRST FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY LAW, THE FIRST REAL BUILDING BLOCKS FOR THAT LEGISLATION WERE LAID A DECADE BEFORE THAT.

The Williams Commission on Freedom of Information and Individual Privacy was appointed in March 1977. The three-volume set of recommendations the Commission presented to the provincial government a little more than three years later in August 1980 were ultimately used as the foundation for Ontario's *Freedom of Information and Protection of Privacy Act*, which passed third reading on June 25, 1987 and received Royal Assent four days later. The *Act* came into effect January 1, 1988.

Another key development started with a phone call in the summer of 1987 to Justice Sidney Linden from then-Attorney General, Ian Scott. Justice Linden, a lawyer who had earlier served as the first Police Complaints Commissioner for Metropolitan Toronto, was then executive director of the Canadian Autoworkers pre-paid legal services plan, the first privately funded national pre-paid legal services plan in Canada.

The string of "firsts" for Justice Linden would continue. The phone call from the Attorney General was an invitation to meet with him. At that meeting, Justice Linden was offered the opportunity to become Ontario's first Information and Privacy Commissioner. (The Attorney General had discussed the appointment with representatives of the two opposition parties before offering it to Justice Linden.)

"I was very enthused about this opportunity," Justice Linden recalled recently. He started that summer on a contract basis, building a small team that had to quickly prepare for the *Act* coming into effect just a few months later. "It was an interesting, challenging and exciting time. We had a small period of time to refine the processes."

One of his early decisions would continue to have an impact two decades later.

The newly appointed Commissioner "really didn't want oral hearings" for every appeal of decisions made by government institutions responding to freedom of information requests, because of his concern that this would delay the appeal process. Instead, he set up a process for written submissions from both the appellant and the government organization. "This was a good success."

Among his key staff in those early days was Ann Cavoukian, the current Commissioner, who joined the small start-up team as the first Director of Compliance in those 1987 early days and who was appointed Assistant Commissioner of Privacy in 1990.

Justice Linden, who had been appointed to a five-year term, expected to complete that term until Attorney General Scott came calling again. In April 1990, he was appointed as Chief Justice of the newly reorganized Ontario Court of Justice (Provincial Division).

Justice Linden, who is now serving as Ontario's Conflict of Interest Commissioner, was asked recently what he thinks of the role of the Information and Privacy Commissioner today. "Information and privacy are very important subjects and have gotten even more important to our democratic system of government 20 years on .... The agency has been very fortunate that good people picked it up and took it to another level."

Here are just a few of the milestones of the first 20 years of Freedom of Information and Protection of Privacy legislation in Ontario. The thousands of phone calls the IPC deals with each year, the long lists of meetings, media interviews, research and policy development, privacy investigations and appeals, speeches and other presentations, all the work that goes into our website, etc., cannot be addressed properly in this chronology. A few of the key events, submissions, policy papers, investigation reports and orders were chosen simply to give you a small glimpse into the type of work that goes on at the IPC.

IPC Chronology – 1987 to 2007

1987

Ontario's *Freedom of Information and Protection of Privacy Act (FIPPA)* passes

- The *Act* passed third reading on June 25, and received Royal Assent on June 29.

Justice Sydney B. Linden appointed as first Commissioner

- He would serve for nearly three years, leading a small team in carving out the office's role and developing jurisprudence (the IPC's early orders set the standards for government organizations to follow).

1988

The *Freedom of Information and Protection of Privacy Act* came into force January 1, 1988

- The *Act*, which gives individuals the right to request access to government-held information, including general records and records containing their own personal information, and requires that the government protect the privacy of an individual's personal information held in government records, came into effect on the first day of the year.
- The first IPC orders were issued and the first investigations conducted into privacy complaints.

1989

The *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* passes

- Ontario's second freedom of information and protection of privacy *Act* (which covers the local government sector) received third reading on December 14, and received Royal Assent the same day. The *Act* would come into effect just over a year later, on January 1, 1991.

The IPC undergoes major organizational restructuring

- After its first full year in operation, the IPC launched a major organizational restructuring to meet its multiple mandates, including the pending implementation of the *Municipal Freedom of Information and Protection of Privacy Act*.

1990

Released the publication, *HIV/AIDS: A Need for Privacy*

- This publication – a good example of how the IPC produces publications that help focus attention on specific access or privacy issues – included information about the flow of HIV/AIDS-related information in the Ontario public health sector, the potential consequences of disclosing HIV/AIDS-related personal information, and discussed such issues as anonymous testing, mandatory reporting, and contact tracing.

Health Cards and Numbers Control Act passes

- This is an example of legislation being brought in after the IPC stressed to the government the need for such a law (in this case, to control the use of the new provincial health numbers in both the public and private sectors).

1991

Tom Wright succeeds Justice Linden as Commissioner

- Tom Wright, who was serving as the Assistant Commissioner (Access), was appointed as Ontario's second Information and Privacy Commissioner.

The *Municipal Freedom of Information and Protection of Privacy Act* comes into force January 1, 1991

- The municipal *Act* is very similar to the provincial *Act* but it covers local government organizations, including municipalities, police services and school boards, instead of provincial organizations. It gives individuals the right to request access to information held by local government organizations, including general records and records containing their own personal information, and it requires that these organizations protect the privacy of the personal information they hold.

1992

IPC submission to the Ontario Telephone Services Commission on adopting recommendations for protecting caller privacy

- When the call-display feature on telephones first came into widespread public use, the IPC was concerned that it may result in individuals losing control of their personal information. The IPC made recommendations to the Ontario Telephone Services Commission to ensure that the then-current levels of privacy could be maintained, through features such as call-blocking.

Caller-ID Guidelines for government organizations published

- These *Guidelines* were issued by the IPC to alert government organizations to the privacy concerns connected with Caller-ID technology and offer direction on how to address them.

1993

Release of *Workplace Privacy: The Need for a Safety Net*

- This publication, which examined workplace privacy issues, called upon the Government of Ontario to establish minimum workplace privacy standards focusing on three issues: (1) electronic monitoring; (2) employee testing; and (3) employment records.

1994

IPC proposes changes to both the provincial and municipal *Freedom of Information and Protection of Privacy Acts* in a submission to the Legislative Assembly committee

- The recommendations were made as part of the three-year review of the municipal *Act*. The IPC called on the government to extend both access and privacy laws to a wider set of public organizations in order to make important public bodies such as hospitals, universities and social services agencies more accountable to the public.

1995

Privacy-Enhancing Technologies: The Path to Anonymity, the first of two joint papers produced by the IPC and the Dutch Data Protection Authority, is published

- This groundbreaking paper looked at how technology could be used to help protect privacy. A joint study had examined leading technologies that allowed anonymous but authenticated transactions – such as blind digital signatures, digital pseudonyms and the use of trusted third parties.

The IPC's website is launched

- The IPC launched its website to provide an additional source of information to the public about access and privacy.

Record set for number of FOI requests

- The number of freedom of information requests filed across Ontario – 26,316 – set a new record. (That record, after additional user fees were introduced the following year, would stand for seven years. New records have been set, however, in four of the past five years, including the 38,584 FOI requests filed in 2007.)

Impact of the *Acts* reduced

- The Labour Relations Act and Employment Statute Law Amendment (often still referred to as Bill 7) was given Royal Assent. It removed certain types of records relating to labour relations or the employment of individuals from the scope of the *Acts*. As a result, public sector employees were precluded from obtaining access to labour relations or employment-related records about themselves, and from making a privacy complaint related to the collection, use or disclosure of their employment-related personal information

1996

Fees for FOI requests expanded

- The Savings and Restructuring Act further amended *FIPPA* and *MFIPPA*, bringing in additional fees. As well, a number of procedural processes were changed and government organizations were given the authority to refuse access in certain circumstances to records on the basis that a request was frivolous or vexatious.

ORDER P-1190 – Ontario Hydro

- Ontario Hydro received a request from a newspaper reporter for access to the most recent internal evaluation reports prepared in response to peer reviews undertaken at each of its nuclear plants. The reports addressed regulatory compliance and supplemented periodic reviews undertaken by the Atomic Energy Control Board. After Hydro denied access to the records on the basis that their disclosure could reasonably be expected to prejudice the economic interests or competitive position of Hydro, the reporter appealed the decision to the IPC. Then-Assistant Commissioner Tom Mitchinson found that a compelling public interest in the disclosure of records concerning nuclear safety existed and that this interest was sufficiently compelling to outweigh the purpose of the section 18(1)(c) exemption cited by Hydro.

1997

Dr. Ann Cavoukian appointed as Commissioner

- Dr. Cavoukian, who had served as the IPC's first Director of Compliance, then as Assistant Commissioner (Privacy), was appointed as Commissioner, and has since gone on to become the first Commissioner ever to be reappointed to a second term. She has served as Commissioner for more than half of the IPC's first 20 years.

Identity Theft: Who's Using Your Name?

- This policy paper not only flagged the issue for governments, the public and the media – at a time when the term ID theft was relatively little known – it offered a number of recommendations on how individuals could protect themselves. This was the first of a number of papers produced by the IPC addressing what has become a major issue.

Drivers can maintain their anonymity on Highway 407

- The IPC worked with the Ontario Transportation Capital Corporation to ensure that the users of the new major electronic toll road, Highway 407, had the option of anonymity (setting up a pre-paid payment account and obtaining a transponder linked to that anonymous payment account).

Order P-1398 – Ministry of Finance

- The Ministry of Finance received a request from a journalist for access to records which evaluated what the economic, social and budgetary implications for Ontario would be if Quebec left Canada. After the request was denied, the reporter appealed the decision to the IPC. Senior Adjudicator John Higgins determined that the compelling public interest in those portions of the records that were subject to the exemptions in sections 13(1) (which governs information qualifying as advice or recommendations) and 15(a) (which protects from disclosure information related to the conduct of intergovernmental relations) was sufficiently strong to outweigh the purpose of these exemptions and the information was ordered released. (He also found that certain information which addressed Ontario's strategic planning and the economic impact on particular sectors of the economy in the event of Quebec separating from Canada was properly exempt under the section 18(1)(d) exemption and that the public interest in the disclosure of this information was not sufficiently compelling to clearly outweigh the purposes of the section 18(1)(d) exemption.)

1998

IPC convinces Ministry of Education to add freedom of information and protection of privacy to the curriculum being developed for new Grade 10 Civics program

- The Ministry of Education was in the process of developing new curriculum for a number of grade levels and the IPC's Tribunal and Communications departments put together a proposal that was presented to the ministry in a face-to-face meeting with senior curriculum officials. The IPC continued to provide input throughout the consultation process for the new curriculum. The IPC was successful in having access and privacy not only added to the Civics curriculum, but placed in the "Specific Expectations" of what students would learn by the end of the course. As this Grade 10 subject is mandatory, every student in Ontario will learn about the significance of freedom of information and protection of privacy.

Start of *Ask an Expert* and special *Teachers' Guides* programs

- The IPC also started to develop teachers' guides on access and privacy for both Grade 5 (the first level where students study government) and Grade 10 (the Civics program). As an adjunct to this, work also began on a program – *Ask an Expert* – under which IPC speakers would address Grade 5 classes.

History in the Making ...

1987

FIPPA

Ontario's first freedom of information and protection of privacy law is passed.

First Commissioner

Justice Sydney B. Linden is appointed as Ontario's first Information and Privacy Commissioner.

1988

Protection Begins

FIPPA, which covers provincial ministries and a number of provincial commissions and agencies, comes into effect January 1, 1988.

1991

MFIPPA

The *Municipal Freedom of Information and Protection of Privacy Act* – which covers the local government sector – comes into effect January 1, 1991.

Tom Wright Appointed Commissioner

Tom Wright, who was serving as the Assistant Commissioner (Access), is appointed as the second Information and Privacy Commissioner.

1997

Ann Cavoukian, Ph.D.

Dr. Cavoukian is appointed as Commissioner and has since gone on to become the first Commissioner ever to be reappointed to a second term.

1997

Biometrics & Privacy

After extensive input from the IPC, the Social Assistance Reform Act is passed with provisions "representing the most rigorous legislative framework in existence for the deployment of a biometric by a government agency," said Commissioner Cavoukian.

1998

Guides for Teachers

The IPC started work on its popular teachers' guides – *What Students Need to Know about Freedom of Information and Protection of Privacy* – for Grade 5 social studies teachers and Grade 10 civics teachers.

2004

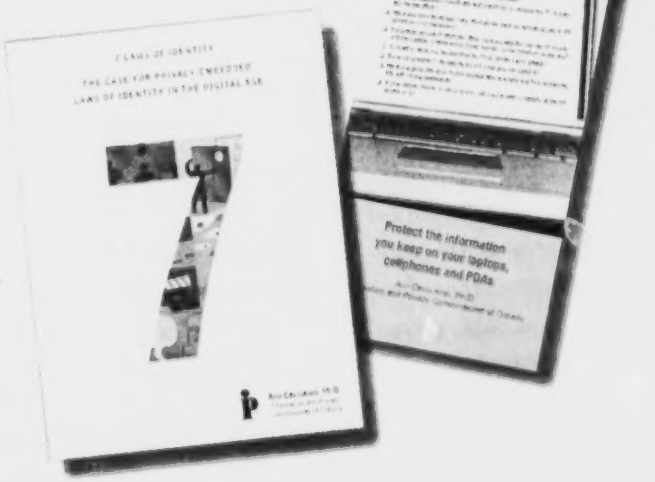
PHIPA

The *Personal Health Information Protection Act*, governing the collection, use and disclosure of personal health information within the health sector, comes into force November 1, 2004.

2006

When Online Gets Out of Line

The brochure above was the first of several IPC publications devoted to the privacy issues related to Facebook and other online social networking sites.



2007

Safeguarding Information

Safeguarding Privacy in a Mobile Workplace is another example of the "how to," practical publications the IPC is developing and issuing.

2006

7 Privacy-Embedded Laws of Identity

The IPC releases an important blueprint for a privacy-enhanced global identity infrastructure to fight excessive disclosure of personal information and online fraud.

1999

Reaching Out to Ontario (ROTO) program launched

- To help the public learn more about its access and privacy rights, the IPC launched its *ROTO* educational initiatives program in the fall of 1999, with a series of presentations, seminars and public meetings (led by the Commissioner) in London, St. Thomas and Chatham over a period of three days. Since then, small IPC teams have visited more than 20 cities or regions across Ontario, several of them twice.

2000

Province of Ontario Savings Office – A Special Report to the Legislative Assembly of Ontario on the Disclosure of Personal Information

- Commissioner Cavoukian tabled a special report in the Legislature based on an investigation by the IPC into an incident involving account holders of the Province of Ontario Savings Office (POSO). An IPC investigation had revealed that the account numbers and account balances of POSO customers, their Social Insurance Numbers and their names and addresses, were provided to the Privatization Secretariat and two private sector firms that were assisting it in reviewing whether government involvement in certain businesses was still warranted. The IPC concluded that the disclosures of this information from POSO to the Privatization Secretariat and from the secretariat to the two firms were not in compliance with *FIPPA*. In a special addendum, the Commissioner was very critical of the Ministry of Finance, the ministry responsible for POSO. "... the Ministry of Finance engaged our Office in a series of protracted discussions designed, in our view, to restrict the scope of our investigation and the investigative tools available to us ..." The detailed information set out in the addendum sparked an emergency debate in the Legislature that lasted several days. That was the first – and last – time the Commissioner had to raise such concerns.

2001

Guidelines for Using Video Surveillance Cameras in Public Places is released

- These detailed *Guidelines* were developed to assist municipalities and police forces considering using a video surveillance system in public areas. The *Guidelines* raised questions about whether such cameras were needed or if the goal could be accomplished otherwise, and outlined how specific privacy protections should be built in if the decision was to proceed with such a system. (The *Guidelines* were subsequently updated in 2007.)

Impact on privacy after the 9-11 attacks reviewed

- Commissioner Cavoukian repeatedly raised concerns she had with the new federal Anti-terrorism Act (part of the Canadian government's response to the terrorists' attacks in New York and Washington on September 11). "... it is important to remember that the goal of these efforts is to protect our democratic society and its citizens – not to create a state in which people fear for their privacy as much as their security, or one where public openness, transparency and accountability are swept aside under the misguided view that these fundamental democratic principles must be subservient to the needs of security."

Launching of STEPs – Security Technologies Enabling Privacy

- This initiative was launched by the Commissioner to convince governments, law enforcement agencies and security vendors that security measures did not automatically have to violate people's privacy in order to be effective.

IPC investigates the use of biometric face recognition technology in Ontario casinos

- The IPC was contacted by a reporter seeking information about the use of biometric facial recognition technology by the Ontario Provincial Police in Ontario's three commercial casinos. The IPC immediately launched an investigation, which determined that the OPP were not scanning the faces of all casino patrons, just those acting "suspiciously," whose faces were then compared to those in a pair of databases. (The facial recognition system used by the OPP was a form of biometric technology that utilized two databases: one of known and suspected casino cheats throughout North America – supplied by a private company – and another, maintained by the OPP surveillance team at each casino, containing the faces of casino cheats convicted in Ontario.) The Commissioner concluded that the OPP's collection of personal information through this program complied with *FIPPA*, but she recommended that the Alcohol and Gaming Commission of Ontario post clearly visible signs at all casinos to notify patrons that video surveillance and facial recognition technology were in use.

2002

Unauthorized access to patient records at University Health Network assessed

- The IPC was contacted in May by the Chief Executive Officer of the University Health Network (UHN) – consisting of three major Toronto hospitals – who asked the Commissioner to conduct a privacy assessment of a certain hospital's response to an apparent breach of patient privacy. (This was in the pre-*PHIPA* days when the health sector was not covered by an Ontario privacy law.) The breach occurred when two well-known Canadians, including one connected to the Toronto Maple Leafs, separately checked into the hospital system for treatment. When UHN ran audits on the electronic health records of the two patients, it discovered that a small number of staff and medical residents had accessed these records, even though they did not appear to be involved in their care. In its review, the IPC concluded that UHN had made considerable efforts to ensure that similar privacy breaches would not happen again. Among the steps taken, UHN conducted a series of inquires and took disciplinary action against the staff that had inappropriately accessed the electronic patient records.

2003

Commissioner Cavoukian named as *Privacy Manager of the Year*

- The Privacy Manager newsletter announced that it had selected Commissioner Cavoukian as *The Privacy Manager of the Year* for 2003. "Many privacy leaders from around the world were nominated," said Publisher Robert Vinet, when making the announcement. "But the one name that kept coming up was that of Dr. Cavoukian .... We looked at all the nominees, and the one person who was head and shoulders above the rest was Dr. Cavoukian."

Mobile Licence Plate Recognition system – Toronto Police Services Board

- A Toronto newspaper reported that the Toronto Police Services Board was undertaking a pilot project testing the Mobile Licence Plate Recognition (MLPR) system, which included video cameras mounted on police cars that scanned the licence plate numbers of parked cars, which the system then compared to a "hot list" of stolen vehicles. The Commissioner initiated an investigation which determined that the operation of the system was in accordance with *MFIPPA*. However, the investigation also determined that the police did not have a contract with the supplier of the MLPR system, even though licence plate numbers were being disclosed to the company by the police. The Commissioner stressed that, in future, the police should

sign a contract containing strong privacy-protection clauses with any private sector business to which the police disclosed personal information. The IPC report also expressed strong concerns about the potential linkage of the MLPR system with global positioning system (GPS) technology. The Commissioner warned that any proposal to use the GPS-configured system would be placed under a high level of scrutiny and that the IPC would oppose any attempt to use the system to track and record the movements of law-abiding citizens.

Hydro One and Ontario Power Generation brought under *FIPPA*

- When Ontario Hydro (which was subject to *FIPPA*) was divided earlier by the government into two large companies and several small ones, the two large companies – Hydro One and Ontario Power Generation – were left outside of *FIPPA*. After strong encouragement from the IPC, both were brought under *FIPPA* by the government in 2003.

IPC releases major report: *What to do if a privacy breach occurs: Guidelines for government organizations*

- These *Guidelines* were published to assist government organizations, but could be used by all organizations. They provide guidance on how to identify and contain a privacy breach, whom to notify, and proactive steps to take to avoid future breaches.

2004

Release of *Blueprint for Action*

- In the *Blueprint for Action* contained in her Annual Report, Commissioner Cavoukian made a series of recommendations designed to promote open, transparent government and the protection of individual privacy in Ontario. To the recently elected government, she emphasized the importance of a central message being delivered to all levels of the Ontario government. In response, within hours of the release of this Annual Report in June 2004, the Premier issued a memorandum to all ministers and deputy ministers calling upon them, "to strive to provide a more open and transparent government."

The *Personal Health Information Protection Act (PHIPA)* comes into force

- *PHIPA* – the first new privacy *Act* in Ontario in nearly 14 years – came into force on November 1, 2004, after substantial input from the IPC. The law governs the manner in which personal health information may be collected, used and disclosed within the health-care system. It also regulates individuals and organizations that receive personal health information directly from health information custodians. Further, *PHIPA* sets out in law a patient's right to access one's own medical records, with very limited exceptions.

Thousands of cheques mailed out containing the personal information of others

- Commissioner Cavoukian tabled a special report with the Legislative Assembly on December 16 after investigating the disclosure of personal information by the Shared Services Bureau (SSB) of Management Board and the Ministry of Finance. Approximately 27,000 Ontario Child Care Supplement for Working Families cheques had been mailed out with counter-foils (cheque stubs) that contained the name and Social Insurance Number (SIN) of the recipient as well as the SIN (along with four additional digits) of another recipient. The Commissioner concluded that the breach was a consequence of a computer system enhancement to the payment-processing application and that the disclosures were clearly not in compliance with *FIPPA*. Among the recommendations made by the Commissioner – as well as a change in the testing process – was that MBS initiate an independent, end-to-end audit of SSB's functions, operations and privacy practices involving the handling of

personal information. (In her 2005 Annual Report, the Commissioner reported that MBS delivered a completed audit that concluded that, as a result of increased efforts, the SSB was addressing privacy in a positive and proactive manner. MBS was also implementing another recommendation by the Commissioner to discontinue use of the SIN.)

2005

Adoption Information Disclosure Act is passed

- In March 2005, Commissioner Cavoukian strongly urged the government to amend its proposed *Adoption Information Disclosure Act*, stressing that birth parents and adoptees from adoptions that had occurred prior to the final passing of this retroactive law be given the right to, if desired, file a disclosure veto to prevent the opening of their sealed files. The *Act* was ultimately passed without Commissioner Cavoukian's proposed disclosure veto. (However, in September 2007, the Ontario Superior Court ruled that the *Act* was unconstitutional. "People expect," said the Court, "and are entitled to expect, that the government will not share [confidential personal] information without their consent. The protection of privacy is undeniably a fundamental value in Canadian society, especially when aspects of one's individual identity are at stake." The Premier did not appeal the ruling and a new version of the law – with the disclosure veto advocated by the Commissioner included – was subsequently introduced for first reading in the Legislature in late 2007.)

IPC presented with the *Privacy Innovation Award*

- The IPC was presented with the *Privacy Innovation Award* by the International Association of Privacy Professionals and Hewlett-Packard for its innovative work, including the development of short, easy-to-understand notices to the public about the new health information privacy law. (Usually, notices about new privacy legislation – often written to address any possible legal development – are lengthy and very hard for the average person to understand. The IPC's much more effective notice system, developed with the assistance of the Ontario Bar Association, includes colourful and very pertinent posters that can be hung on office walls, as well as easy-to-read brochures that explain information practices.)

First Health Order issued under *PHIPA*

- This order, following an investigation by the Commissioner into personal health records being strewn across Toronto streets as a backdrop to a film production, established new standards for the secure destruction of personal information. (The records tossed onto the streets were to have been destroyed by a shredding company but were inadvertently sold by its recycling arm as scrap paper to the film company.)

Order MO-1947 – City of Toronto

- A reporter sought access to information relating to lawsuits filed against four departments within the City of Toronto that were settled between 1998 and 2004. Access to the responsive records was denied, with the city citing exemptions in the municipal *Act* (sections 11(c) and (d)) that address information whose disclosure could prejudice the city's financial or economic interests, or its competitive position. After that decision was appealed to the IPC, the Commissioner ultimately concluded that the city had failed to provide the kind of detailed and convincing evidence required to establish the harms outlined in section 11. Commissioner Cavoukian reiterated the need for open and transparent government, particularly where the information sought relates to the expenditure of public funds. She encouraged the city to follow through on a commitment by Mayor David Miller to develop a culture of openness rather than one based on a "protective mindset."

Order PO-2435 – Ministry of Health and Long-Term Care

- The ministry received a request for all the records pertaining to the province's e-Physician Project (including the Smart Systems for Health Agency), which consisted of various requests for proposals, contracts, invoices and so on related to the consultants hired for the project. The ministry applied the mandatory third party information exemption in section 17(1) of the *Act* to the records. Assistant Commissioner Brian Beamish found that the information contained in service contracts entered into between the ministry and its consultants and other documents that referred to the same information were not "supplied" to it, as they had been the subject of negotiation. As a result, the information could not be exempted from disclosure under section 17(1). He also went on to evaluate whether the harms test in section 17(1) had been successfully established and found that it had not. Assistant Commissioner Beamish emphasized the need for public accountability in the expenditure of public funds as an important reason behind the need for "detailed and convincing evidence" to support the harms outlined in section 17(1).

2006

First *Right to Know Week* held

- *Right to Know Week* is based on the international *Right to Know Day*. On September 28, 2002, freedom of information organizations from various countries (primarily from Europe) met in Sofia, Bulgaria, created a network of Freedom of Information Advocates, and agreed to collaborate in the promotion of open government. *Right to Know Week* in Canada, launched by provincial and territorial Information and Privacy Commissioners and the federal Information Commissioner, builds on that theme. The week highlights the importance of Canada's various freedom of information regimes. The IPC put together a special panel discussion for what quickly became a sold-out luncheon. Two panelists from the media and a moderator and panelist from the IPC discussed the importance of open government. (The IPC more than doubled the size of the facility for the 2007 panel discussion it organized, attracting another standing-room-only crowd.)

Privacy and Data Protection Commissioners around the world accept the Global Privacy Standard

- International Privacy and Data Protection Commissioners accepted the Global Privacy Standard (GPS) that a committee of international commissioners – which Commissioner Cavoukian chaired – developed and brought forward. The GPS represents a harmonization of fair information practices into a single instrument, and for the first time, includes the explicit language of data minimization.

The Divisional Court affirms for the first time that the Commissioner has the authority to investigate and report on privacy complaints made by the public against government institutions

- At the same time, the Court held that the Commissioner's privacy rulings were protected by "Parliamentary privilege" and were not subject to judicial review by the Courts because they fell within the general oversight and reporting mandate of the Commissioner – as an Officer of the Legislature.

Universities placed under the *Freedom of Information and Protection of Privacy Act*

- As repeatedly advocated by the IPC, universities (as they are in a number of other provinces) were brought under *FIPPA* on June 10, 2006.

The privacy implications of online social networking

The IPC, partnering with Facebook, produces the first of several hands-on, practical publications addressing the privacy implications of the rapidly growing online social networking trend.

2007

Court ruling strikes down bylaw

- In July, the Ontario Court of Appeal struck down a City of Oshawa bylaw that had required used-goods retailers to collect extensive personal information from people who wanted to sell one or more second-hand items to such stores. This personal information, including a photograph and the particulars of three pieces of government-issued identification, was to then be transmitted to, and stored centrally in, a police database, without any restrictions on its use or judicial oversight.

MO-2225 – City of Ottawa ruling sets precedent

- Commissioner Cavoukian – invoking for the first time a cease collection and destroy records provision in Ontario privacy laws – ordered the City of Ottawa and the Ottawa Police to stop collecting extensive personal information from individuals selling used goods to second-hand stores. She also ordered the destruction of personal information already collected. (For more details, please see the *High Profile Privacy Incidents* chapter in this Annual Report.)

Two key IPC decisions upheld

- In July, an Ontario Divisional Court's ruling upheld two decisions made by the IPC on the application of the solicitor-client exemption to legal fees. The ruling was a strong endorsement of the IPC's approach to the disclosure of legal fee information under *FIPPA* and *MFIPPA*. (For more information on this and the next highlight, please see the *Judicial Reviews* chapter in this Annual Report.)

'Public interest override' provisions expanded

- Also in 2007, the Court of Appeal issued a very significant decision involving an appeal by the Criminal Lawyers Association. The Court granted the appeal, significantly expanding the circumstances upon which the "public interest override" provision in the provincial and municipal *Freedom of Information and Protection of Privacy Act* may apply.

Release of a key research paper, *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy*

- Co-authored by the Commissioner and Alex Stoianov, Ph.D., this research paper sets out the privacy, security and trust problems related to biometric information systems and explains how an emerging new technology, biometric encryption, can address those concerns. "BE technology," said the Commissioner, "not only holds the promise of superior privacy and personal control for individuals over their own biometric data, but also stronger information security and greater user confidence and trust in biometric identification systems." (For more information, please see the *Advancing Privacy through Technology* chapter in this Annual Report.)

NEW RECORD SET

38,584 FOI Requests

filed across Ontario in 2007

Requests by the Public

EARLY EACH YEAR, PROVINCIAL AND MUNICIPAL GOVERNMENT ORGANIZATIONS ARE REQUIRED UNDER THE *ACTS* TO REPORT TO THE IPC ON THE NUMBER OF REQUESTS FOR INFORMATION OR CORRECTION OF PERSONAL INFORMATION THEY RECEIVED DURING THE PAST CALENDAR YEAR, AS WELL AS TIMELINESS OF RESPONSES, OUTCOMES AND FEES COLLECTED.

There were 38,584 freedom of information (FOI) requests filed across Ontario in 2007. This is the greatest number of requests ever filed, breaking the previous record of 36,739 set in 2006.

Provincial government organizations received 14,281 FOI requests in 2007, a 1.5 per cent increase over 2006 (when 14,076 requests were filed). Of these, 3,467 (nearly one-quarter) were for personal information and 10,814 (75.7 per cent) were for general records.

Ontario's 19 universities, which were brought under the legislation as of June 10, 2006, received a total of 226 requests in 2007 – their first full year subject to FOI. (See the universities chart in the *Response Rate Compliance* chapter.)

Municipal government organizations received 24,303 requests in 2007, a 7.2 per cent increase over 2006 (when 22,663 requests were filed). Of these, 9,857 (just over 40 per cent) were personal information requests and 14,446 (just under 60 per cent) were for general records.

The Ministry of Environment once again received the largest number of requests under the provincial *Act* (6,094), followed by the ministries of Community Safety and Correctional Services (3,477), Labour (990) and Community and Social Services (707). Together, these four ministries received nearly four out of every five provincial requests (78.9 per cent).

Police Services Boards received the most requests under the municipal *Act* – 13,437 (slightly over 55 per cent). Municipal corporations were next with 10,259 (just over 42 per cent), followed by school boards (210 requests, slightly under one per cent) and electricity corporations (199, also just under one per cent).

The majority of provincial requests in 2007 (just over 71 per cent) were made by businesses, while individuals made the majority of municipal requests (slightly over 68 per cent).

The *Acts* contain a number of exemptions that allow, and in some situations actually require, government organizations to refuse to disclose requested information. In 2007, the most frequently cited exemptions for personal information requests were the protection of other individuals' privacy, followed by law enforcement. Privacy protection was also the most-frequently cited exemption for general records requests, followed by law enforcement.

The *Acts* give individuals the right to request correction of personal information about them that is held by government organizations. In 2007, provincial organizations received five requests for corrections and refused four. Municipal organizations received 22 correction requests and refused four.

When a correction is refused, the requester can attach a statement of disagreement to the record, outlining why the information is believed to be incorrect. There were four statements of disagreement filed with municipal organizations.

The legislation provides for a number of fees. In addition to the mandatory $5 application fee, government organizations can charge certain prescribed fees for responding to requests. Where the anticipated charge is more than $25, a fee estimate can be given to a requester before search activity begins.

Organizations have discretion to waive fees where it seems fair and equitable to do so, after weighing several specific factors listed in the *Acts*.

Provincial organizations reported collecting $68,808.18 in application fees and $453,876.34 in additional fees in 2007. The corresponding numbers for municipal organizations were $120,192.68 and $302,022.59.

Search fees were the most commonly charged fees by provincial organizations (just over 57 per cent – compared to nearly 64 per cent in 2006), followed by reproduction costs (nearly 20 per cent) and shipping charges (12 per cent). Municipal organizations, by contrast, most frequently charged for reproduction (nearly 29 per cent), followed by search fees (just over 28 per cent) and preparation costs (26.5 per cent).

The average cost of FOI requests dropped slightly at the provincial level and rose slightly at the municipal level, though the average provincial fees were still substantially higher than municipal ones. The highest average fee was in the general records category under the provincial *Act*: $50.54, compared to $51.11 the previous year. (See the accompanying chart.)

Outcome of Requests – 2007

PROVINCIAL REQUESTS

MUNICIPAL REQUESTS

Fees Collected – 2007

	Provincial $	Municipal $
Total Application Fees Collected	68,808.18	120,192.68
Total Additional Fees Collected	453,876.34	302,022.59
Total Fees Waived (dollars)	31,968.51	14,350.75

Average Cost of Provincial Requests

	2006 $	2007 $
Personal Information	11.55	10.54
General Records	51.11	50.54

Average Cost of Municipal Requests

	2006 $	2007 $
Personal Information	8.64	9.67
General Records	21.04	23.49

Response Rate Compliance

EACH YEAR, THE IPC REPORTS COMPLIANCE RATES FOR MINISTRIES AND OTHER SELECTED GOVERNMENT ORGANIZATIONS.

Two calculations are made, reflecting the different provisions of the *Acts*. The first shows what percentage of freedom of information requests were responded to within the 30-day standard set by the *Acts*.

The second compliance rate, listed in the tables as Extended Compliance, is the 30-day compliance rate adjusted to factor in Notices of Extension and/or Notices to Affected Person. These notices allow a government organization to be in compliance with the applicable *Act* while taking more than 30 days to respond to a request. They are used in circumstances where, for example, there is a need to search through a large number of records or consult with one or more people outside the organization.

Notices of Extension are explained in more detail in section 27(1) of the provincial *Act* and section 20(1) of the municipal *Act*. The corresponding sections for Notices to Affected Person are 28(1) and 21(1).

One Part of the Story

Since the IPC began emphasizing the importance of response times, the provincial 30-day compliance rate has climbed dramatically from 42 per cent to more than 80 per cent.

While this is a positive indicator, it is important to understand that the response rate alone does not indicate that a particular government organization is doing an excellent job when it comes to freedom of information (FOI). For example, an institution may respond in a timely way but deny access to what should be routinely available information. Or it may include an unreasonably high fee estimate, or some other response that frustrates the intent of the applicable *Act*.

It is important that institutions adhere not only to the letter of the *Act* but also its spirit, which includes accountability, transparency, and openness.

Institutions Governed under the Provincial *Act*

Ministries, agencies and other institutions under the provincial *Act* achieved a record 30-day compliance rate of 84.8 per cent in 2007. This is the highest percentage since the inception of the provincial *Act* 20 years ago and a big improvement over the 73.5 per cent achieved in 2006.

The extended compliance rate also set a record at 92 per cent, up from 86.5. (This figure has only been calculated since 2002.)

The accompanying provincial chart lists ministries and agencies ranked by the number of requests completed in 2007. As usual, the Ministry of the Environment completed by far the most requests – 5,988. Of these, 84.4 per cent were completed within 30 days, a sharp increase of more than 20 percentage points from the previous year. With notices, the ministry's compliance rate was 87 per cent, up significantly from 76.5 per cent in 2006.

The Ministry of Community Safety and Correctional Services was the only other ministry that completed more than 1,000 requests. It completed an even 3,400 in 2007. Of these, 82.8 per cent were completed within 30 days, up slightly from 81.2 in 2006. It recorded the same excellent extended compliance rate – 97.8 per cent – as the previous year.

RESPONSE RATE COMPLIANCE

Provincial Institutions

(includes organizations where the Minister is the Head)
(ranked by number of requests completed in 2007)

			Within 1-30 Days		Extended Compliance*
	Requests Received	Requests Completed	No.	%	%
Environment	6090	5988	5056	84.4	87.0
Community Safety and Correctional Services	3477	3400	2814	82.8	97.8
Labour	875	880	810	92.0	96.1
Community and Social Services	707	667	606	90.9	94.0
Government and Consumer Services	429	440	400	90.9	94.0
Transportation	333	321	296	92.2	99.4
Attorney General	343	308	279	90.6	98.7
Health and Long-Term Care	131	144	80	55.6	72.9
Natural Resources	129	120	60	50.0	85.0
Finance	84	82	63	76.8	93.9
Training, Colleges and Universities	64	63	44	69.8	88.9
Revenue	51	59	47	79.7	96.6
Municipal Affairs and Housing	47	49	46	93.9	98.0
Children and Youth Services	39	42	37	88.1	95.2
Education	35	40	35	87.5	90.0
Agriculture, Food and Rural Affairs	30	28	19	67.9	92.9
Cabinet Office	25	22	22	100.0	100.0
Energy	16	17	7	41.2	41.2
Public Infrastructure Renewal	20	17	11	64.7	70.6
Citizenship and Immigration	11	11	8	72.7	100.0
Culture	10	10	9	90.0	100.0
Economic Development and Trade	6	10	5	50.0	90.0
Aboriginal Affairs	6	8	4	50.0	50.0
Health Promotion	6	8	4	50.0	50.0
Intergovernmental Affairs	7	7	7	100.0	100.0
Northern Development and Mines	4	4	3	75.0	100.0
Tourism	2	3	2	66.7	100.0
Francophone Affairs	1	2	2	100.0	100.0
Research and Innovation	0	1	0	0.0	100.0
Small Business and Entrepreneurship	1	1	1	100.0	100.0

**Including Notice of Extension, section 27(1), and Notice to Affected Person, section 28(1). Such notices are used in circumstances where, for example, there is a need to search through a large number of records or consult with one or more people outside the organization.*

Universities

Amendments to the *Freedom of Information and Protection of Privacy Act* made Ontario's universities subject to the *Act* midway through June 2006. 2007 was the first full year for these institutions under the legislation.

The total number of completed requests by universities in 2007 was 214, up from the 139 completed during the last six-plus months of 2006. The University of Ottawa completed 28 of these (having received 41 over the year, significantly more than any other university).

McMaster University and York University were the other two universities with more than 20 completed requests. The University of Windsor achieved a 100 per cent 30-day compliance rate on 14 requests, and Ryerson improved from 12.5 per cent in 2006 to 92.3 per cent in 2007. McMaster finished with a 30-day compliance rate of only 16.7 per cent, but registered an overall 95.8 per cent compliance rate when notices were considered.

Universities

(ranked by the number of requests completed in 2007)

			Within 1-30 Days		Extended Compliance*
	Requests Received	Requests Completed	No.	%	%
University of Ottawa	41	28	21	75.0	100.0
McMaster University	10	24	4	16.7	95.8
York University	19	21	13	61.9	85.7
Carleton University	21	19	13	68.4	100.0
University of Toronto	19	19	18	94.7	100.0
University of Western Ontario	21	19	18	94.7	100.0
Queen's University	21	18	15	83.3	88.9
University of Windsor	14	14	14	100.0	100.0
Ryerson University	16	13	12	92.3	100.0
Laurentian University	6	9	7	77.8	88.9
University of Guelph	7	7	3	42.9	100.0
Trent University	7	7	4	57.1	100.0
Brock University	6	5	5	100.0	100.0
University of Waterloo	4	3	3	100.0	100.0
Lakehead University	6	2	2	100.0	100.0
Nipissing University	2	2	2	100.0	100.0
University of Ontario Institute of Technology	3	2	2	100.0	100.0
Wilfrid Laurier University	2	1	1	100.0	100.0
Ontario College of Art & Design	1	1	1	100.0	100.0

**Including Notice of Extension, section 27(1), and Notice to Affected Person, section 28(1). Such notices are used in circumstances where, for example, there is a need to search through a large number of records or consult with one or more people outside the organization.*

More Statistics Overall

This year, the IPC has changed the way it reports on compliance rates. In addition to the provincial chart and a universities chart, we are publishing – for easier comparison purposes – a municipal chart showing the 30 government organizations under the municipal *Act* that completed the most FOI requests last year.

We are also publishing, on our website, compliance rates for up to the top 50 organizations in each of five local government categories, including police services and school boards. (Some categories do not have 50 organizations that responded to FOI requests in 2007.)

Institutions Governed by the Municipal *Act*

The accompanying *Top 30 Municipal Institutions* chart ranks institutions governed by the municipal *Act* by their number of completed requests. That *Act* covers not just municipalities but also police services, school boards, health boards, etc.

The 30-day compliance rate for this entire group of institutions in 2007 was 86.9 per cent. With notices it was 91.1 per cent. Both figures are up very slightly from 2006.

The City of Toronto, with 5,548 completed requests, was the leader, completing more requests than all but one provincial ministry. In fact, every one of the top 30 municipal institutions completed more requests than two-thirds of the provincial ministries and agencies.

Police services hold the second through eighth places on the top 30 municipal list (and the majority of spots overall, with 19 of the 30). Toronto Police Services recorded a 79.4 per cent 30-day compliance rate (83.1 per cent with notices).

Two police services, Durham Regional and Niagara Regional, posted notable improvements in their compliance rates. Durham improved its 30-day compliance to 80.5 per cent in 2007, from 65.5 per cent in 2006, with the extended compliance percentage climbing to 84.4 from 69.8. Niagara's 30-day

RESPONSE RATE COMPLIANCE

Top 30 Municipal Institutions

(ranked by number of requests completed in 2007)

			Within 1-30 Days		Extended Compliance*
	Requests Received	Requests Completed	No.	%	%
City of Toronto	5203	5548	4746	85.5	88.9
Toronto Police Services Board	3194	3108	2468	79.4	83.1
Hamilton Police Service	1403	1384	1105	79.8	92.3
Peel Regional Police	1077	1075	1074	99.9	99.9
Durham Regional Police Service	979	962	774	80.5	84.4
Niagara Regional Police Service	956	950	848	89.3	97.2
Halton Regional Police Service	905	862	852	98.8	99.8
Windsor Police Service	705	710	580	81.7	95.1
Town of Oakville	636	635	623	98.1	98.9
London Police Service	618	590	415	70.3	97.6
City of Kitchener	511	512	508	99.2	100.0
City of Mississauga	457	445	437	98.2	99.3
Waterloo Regional Police Service	396	380	377	99.2	54.7
Ottawa Police Service	358	368	296	80.4	98.4
City of Ottawa	378	359	302	84.1	89.4
Town of Richmond Hill	345	345	337	97.7	100.0
City of Brampton	335	334	331	99.1	99.4
Guelph Police Service	333	327	297	90.8	95.1
Sarnia Police Service	327	323	270	83.6	96.6
Brantford Police Service	309	309	200	64.7	64.7
Barrie Police Service	309	307	304	99.0	99.0
York Regional Police	183	188	158	84.0	87.2
Thunder Bay Police Services	181	182	180	98.9	99.5
South Simcoe Police Service	138	137	96	70.1	73.7
Peterborough Lakefield Police	134	134	134	100.0	100.0
City of Barrie	132	132	119	90.2	90.2
City of Greater Sudbury	123	118	105	89.0	89.8
City of Hamilton	106	111	104	93.7	93.7
Chatham-Kent Police Service	108	108	97	89.8	89.8
Regional Municipality of Peel	98	103	63	61.2	62.1

**Including Notice of Extension, section 20(1), and Notice to Affected Person, section 21(1). Such notices are used in circumstances where, for example, there is a need to search through a large number of records or consult with one or more people outside the organization.*

percentage was 89.3, up from 76.6, while the extended compliance percentage was 97.2, bettering 2006's 83.2 per cent.

School Boards

School boards were again led in 2007 by the District School Board of Niagara, which completed 67 access requests, down slightly from 2006's 74. The board posted an 88.1 per cent 30-day compliance rate.

Other boards completing 10 or more access requests were the Dufferin-Peel Catholic District School Board, Toronto District School Board and Thames Valley District School Board.

For More Information

Extended charts of compliance statistics for municipalities (sorted by population), police services and school boards are available as part of a special report on the IPC's website, www.ipc.on.ca. This special report, *Compliance Statistics: A look at the compliance rates of government organizations*, has been posted as an adjunct to the Annual Report.

Access

THE *ACTS* PROVIDE THAT, SUBJECT TO LIMITED AND SPECIFIC EXEMPTIONS, INFORMATION UNDER THE CONTROL OF PROVINCIAL AND MUNICIPAL GOVERNMENT ORGANIZATIONS SHOULD BE AVAILABLE TO THE PUBLIC.

If you make a written freedom of information request under one of the *Acts* to a provincial or municipal government organization and are not satisfied with the response, you have a right to appeal that decision to the IPC.

Records that do not contain the personal information of the requester are referred to as general records. Appeals concerning general records may relate to a refusal to provide access, fees, the fact that the organization did not respond within the prescribed 30-day period, or other procedural aspects relating to a freedom of information request.

When an appeal is received, the IPC first attempts to settle it informally. If all issues cannot be resolved, the IPC may conduct an inquiry and issue a binding order, which may require the government organization to release all or part of the requested information.

Statistical Overview

In 2007, a total of 957 appeals involving general records and personal information were submitted to the IPC. This represents an increase of just over seven per cent from 2006, when 893 appeals were received.

Overall, 873 appeals were closed in 2007.

Access to General Records

Appeals Opened

Overall, 571 appeals regarding access to general records were made to the IPC in 2007. Of these, 316 (just over 55 per cent) were filed under the provincial *Act* and 255 (or about 45 per cent) were filed under the municipal *Act*.

Of the 316 appeals received under the provincial *Act*, 199 (63 per cent) involved ministries and 117 (37 per cent) involved agencies.

There were 32 general information appeals against decisions made by each of the Ministry of Community Safety and Correctional Services, and the Ministry of Health and Long-Term Care. The Ministry of the Environment had the next highest number (27), followed by the ministries of Natural Resources (19), Training, Colleges and Universities (17), and Transportation (16).

The Ontario Lottery and Gaming Corporation had 21 appeals, up from eight the previous year, making it the agency with the greatest number of appeals in 2007. Many of these related to requests that were sparked by a CBC report about the number of store owners and employees who have cashed winning lottery tickets.

Other agencies with a relatively high number of general records appeals included the Ontario Realty Corporation (18), York University (10), Archives of Ontario (nine), McMaster University (seven), and the Office of the Public Guardian and Trustee (six).

Of the 255 general records appeals received under the municipal *Act*, 168 (almost 66 per cent) involved municipalities, 57 (about 22 per cent) involved police services, and 15 (or just under six per cent) involved boards of education. Another 15 appeals (about six per cent) involved other types of municipal institutions.

Issues in General Records Appeals Opened

	Provincial		Municipal		Total	
	No.	%	No.	%	No.	%
Exemptions Only	134	42.4	139	54.5	273	47.8
Third Party	54	17.1	13	5.1	67	11.7
Reasonable Search (sole issue)	37	11.7	27	10.6	64	11.2
Exemptions with Other Issues	23	7.3	13	5.1	36	6.3
Deemed Refusal	23	7.3	11	4.3	34	6.0
Interim Decision	9	2.8	7	2.7	16	2.8
Fee and Fee Waiver	5	1.6	13	5.1	18	3.1
Time Extension	5	1.6	2	0.8	7	1.2
Inadequate Decision	0	0	2	0.8	2	0.4
Frivolous or Vexatious	0	0	1	0.4	1	0.2
Transfer	1	0.3	0	0	1	0.2
Other	25	7.9	27	10.6	52	9.1
Total	**316**	**100**	**255**	**100**	**571**	**100**

Types of Appellants in Appeals Opened

	Provincial		Municipal		Total	
	No.	%	No.	%	No.	%
Individual	127	40.2	165	64.7	292	51.1
Business	118	37.3	55	21.6	173	30.3
Media	38	12	24	9.4	62	10.9
Association/Group	17	5.4	8	3.1	25	4.4
Academic/Researcher	9	2.8	0	0	9	1.6
Government	3	0.9	1	0.4	4	0.7
Union	4	1.2	0	0	4	0.7
Politician	0	0	2	0.8	2	0.4
Total	**316**	**100**	**255**	**100**	**571**	**100**

Outcome of Appeals Closed Other Than By Order

	Provincial		Municipal		Total	
	No.	%	No.	%	No.	%
Mediated in Full	144	62.3	104	57.5	248	60.2
Withdrawn	45	19.5	50	27.6	95	23.1
Other	18	7.8	15	8.3	33	8.0
Screened Out	22	9.5	10	5.5	32	7.8
Abandoned	2	0.9	2	1.1	4	1.0
Total	**231**	**100**	**181**	**100**	**412**	**100**

In terms of the issues raised, 273 (or almost 48 per cent) of general records appeals were related to the exemptions claimed by institutions in refusing to grant access. In 64 (about 11 per cent) of the appeals, the issue was whether the institution had conducted a reasonable search for the records requested.

Thirty-six (6.3 per cent) of the appeals related to exemptions combined with other issues. Another 34 (six per cent) were the result of deemed refusals to provide access, where the institution did not respond to the request within the time frame required by the *Act*. The remaining appeals were related to fees, time extensions, interim decisions and various other issues.

Of the provincial institutions, the Ministry of Health and Long-Term Care had the highest number of deemed refusal appeals, with six. No other ministry or agency had more than two. Of the municipal institutions, the Town of Hawkesbury had two. No other municipal institution had more than one.

Most appellants (just over 50 per cent) were individual members of the public.

Just over 85 per cent of appellants represented themselves. Lawyers (73) or agents (nine) represented appellants in about 14 per cent of the general records appeals made in 2007.

This year, $11,625 in application fees for general records appeals was paid to the IPC and forwarded to the Minister of Finance.

Appeals Closed

The IPC closed 544 general records appeals during 2007. Of these, 292 (almost 54 per cent) concerned provincial institutions, while 252 (about 46 per cent) concerned municipal institutions.

Of the 544 general records appeals closed, 113 (just over 20 per cent) were closed at the intake stage, 252 (about 46 per cent) at the mediation stage, and 179 (or almost 33 per cent) at the adjudication stage.

More than 75 per cent of general records appeals were closed without a formal order being issued. Of these, 248 (about 60 per cent) were mediated in full, 95 (23 per cent) were withdrawn, and 32 (almost eight per cent) were screened out.

Outcome of Appeals Closed By Order

	Provincial		Municipal		Total	
Head's Decision	No.	%	No.	%	No.	%
Not Upheld	10	16.4	16	22.5	26	19.7
Partially Upheld	17	27.9	25	35.2	42	31.8
Upheld	31	50.8	27	38	58	43.9
Other	3	4.9	3	4.2	6	4.5
Total	**61**	**100**	**71**	**100**	**132**	**100**

Nearly one-quarter (132) of general records appeals were closed by an order. The IPC issued 61 provincial and 71 municipal orders related to general records. Thirteen interim orders were also issued, of which eight were provincial and five municipal.

Overall, in appeals resolved by order, the decision of the head was not upheld or only partially upheld in 51.5 per cent of the appeals. The decision of the head was upheld in about 44 per cent of the appeals. The remaining 4.5 per cent had other outcomes.

High Profile Appeals

THE IPC CLOSED 873 APPEALS IN 2007. AMONG THE MOST HIGH PROFILE APPEALS WERE THESE THREE:

Order MO-2237 – Barrie Police Services Board

The appellant's daughter died suddenly in the summer of 2005. At the time of her death, she lived in the City of Barrie and shared an apartment with another individual (the affected party).

The Barrie Police and the Coroner's Office conducted an investigation into the death, including carrying out interviews that were recorded digitally. One of the interviews was with the affected party.

The appellant had made a request for information related to the investigation. The police granted partial access and relied on sections 38(a) and (b) of the *Municipal Freedom of Information and Protection of Privacy Act* to deny access to the remainder. The records at issue in this appeal included the digitally recorded interview with the affected party, a sudden death report, and police officers' notes.

The interview and other undisclosed information consisted of personal information relating to the deceased intermingled with that of the affected party. The appellant raised the possible application of the newly-enacted section 14(4)(c), which provides for the disclosure of personal information relating to a deceased individual to the spouse or close personal relative where "in the circumstances, the disclosure is desirable for compassionate reasons."

Section 14 is relevant in assessing the application of the personal privacy exemption in section 38(b). The principal issue in the appeal was whether section 14(4)(c) permits disclosure of the personal information about the appellant's daughter that is comingled with that of the affected person. If this section applies, the information is not exempt under section 38(b) as its disclosure would not constitute an unjustified invasion of personal privacy.

The adjudicator, Assistant Commissioner Brian Beamish, held that for the purposes of section 14(4)(c), "personal information of a deceased individual" can include intermingled information about another individual. He also found that the privacy interests of other individuals could be a relevant circumstance in deciding whether disclosure was "compassionate."

A three-part test was articulated to assist in determining the applicability of section 14(4)(c). First, it must be determined if the records contain the personal information of the deceased individual. Second, it must be established whether the requester is a spouse or "close relative" of the deceased individual. Third, one must ask whether the disclosure of the personal information of the deceased individual is desirable for compassionate reasons in the circumstances of the appeal.

Assistant Commissioner Beamish adopted two dictionary meanings for the term "compassionate" in this case. They refer to being sympathetic and ascribing to the Legislature an intention to "address an identified gap in the access to information legislation and increase the amount of information being provided to bereaved family members."

Applying these principles, the Assistant Commissioner found that the disclosure of much of the remaining information from the digital recording and the police officers' notebook entries was desirable for compassionate reasons under section 14(4)(c). As a result, its disclosure would not be an unjustified invasion of personal privacy, and thus the information was not exempt from disclosure under section 38(b).

In addition, Assistant Commissioner Beamish ordered the police to sever and withhold those portions of the records that relate only to the affected party and not the deceased individual, wherever possible. He further ordered that the appellant only be given access to the audio portion of the digital recording, in order to minimize the disclosure of the affected party's personal information.

Order PO-2541 – Archives of Ontario

The Archives of Ontario received a request for access to two correctional centre files dating from 1941 which relate to a named individual believed to be the requester's birth father. The requester had received some information from the Adoption Disclosure Registry about his birth father, including his name and the fact that he had been incarcerated at the correctional centre at the time of the requester's birth.

Archives located 19 pages of responsive records and refused to confirm or deny their existence to the requester under section 21(5) of the *Freedom of Information and Protection of Privacy Act*.

The requester appealed this decision to the Commissioner's office. He indicated that he had required access to any medical information that might be in the records relating to his birth father, to assist in the medical diagnosis of a condition suffered by his daughter.

Senior Adjudicator John Higgins first found that the records contained the personal information of the named individual, comprising certain medical information, as well as other information relating to his arrest and incarceration. The senior adjudicator then examined whether the exception to the general prohibition against the disclosure of personal information in section 21(1)(b) applied to the medical information in the records. This section allows for the disclosure of another's personal information in compelling circumstances affecting the health or safety of an individual.

The senior adjudicator found that the compelling circumstances contemplated by section 21(1)(b) had been satisfied and that the medical information in the records ought to be disclosed to the appellant.

He based this finding on the fact that the name of the appellant's birth father is identical to that of the individual who was incarcerated and that the information provided by the Adoption Disclosure Registry is consistent with the information in the records. He concluded that the individual identified in the records was, in fact, the appellant's birth father. Accordingly, the Archives was not permitted to "refuse to confirm or deny" the existence of records under section 21(5) as disclosure of the medical information would not be an unjustified invasion of personal privacy. The senior adjudicator ordered disclosure of the medical information.

Senior Adjudicator Higgins went on to conclude that the remaining information relating to the birth father's arrest and incarceration was not, however, subject to the exception in section 21(1)(b). He found that the other personal information in the records was exempt from disclosure under section 21(1) as its disclosure would result in an unjustified invasion of the birth father's personal privacy.

Order MO-2258 and Privacy Complaint Report MC-060020-1 – Toronto Police Services Board

This order and privacy complaint relate to the appellant's concerns about getting a clear police reference check in connection with volunteer work.

The appellant had been arrested in 2002. The arrest arose from an allegation by his younger brother that he and another individual (a third brother) had sexually assaulted him more than 40 years prior to the arrest. The arrest occurred shortly after the sexual assault allegation was brought to the attention of the Toronto Police Service. As a result, the appellant/complainant was charged with indecent assault on a male pursuant to section 148 of the Criminal Code. The charge was eventually withdrawn by the Crown.

The appellant made an access and correction request to the Toronto Police Services Board under the *Municipal Freedom of Information and Protection of Privacy Act*. The police denied access to some of the requested information (the record of arrest and the occurrence report) and eventually denied the correction request. The appellant appealed and, during the course of the appeal, also submitted a privacy complaint.

Throughout this process, the appellant was engaged in lengthy correspondence with the police, beginning before he made the access and correction request and continuing during the processing of his complaint and appeal based on his concerns about getting a clear police reference check.

The police service indicated to the appellant/complainant that information contained in its Centralized Occurrence Processing System (COPS) relating to his arrest and charge is permanently maintained pursuant to the Toronto Police Service Record Retention Schedule, City of Toronto By-law 689-2000 and cannot, accordingly, be the subject of a correction request under section 36(2)(a) of the *Act*. The police advised him, however, that his photograph and fingerprint records had been destroyed and that the reference to him in the Canadian Police Information Centre (CPIC) database had been removed.

In Order MO-2258, Senior Adjudicator Higgins addressed the issues arising out of the appellant's access request, including the question of whether he is entitled to obtain access to the undisclosed portions of the records and whether he is entitled to have the records corrected and/or destroyed.

Senior Adjudicator Higgins determined that certain portions of the responsive records were not exempt from disclosure under section 38(b) of the *Act* by applying the consent provision in section 14(1)(a) and the absurd result principle. He found that the disclosure of the personal information in the records would not result in an unjustified invasion of personal privacy. Further disclosure to the appellant was therefore ordered.

Next, the senior adjudicator addressed the correction issue. The test for whether to accept or reject a correction request under section 36(2)(a) is whether the record contains personal information that is "inexact, incomplete or ambiguous." The senior adjudicator found that the personal information did not fit this description and that, consequently, section 36(2)(a) did not apply.

In addition, the senior adjudicator addressed and rejected the possibility that section 36(2)(a) must be read in some different fashion so as to ensure that it is consistent with "Charter values." He did, however, point out that this was not to be construed as a finding that the police reference check program complies with the Charter. He noted the particular importance of section 11(a), which provides that individuals charged with offences are entitled to be presumed innocent until proven guilty.

In Privacy Complaint Report MC-060020-1, the senior adjudicator examined whether the collection and retention of the appellant's personal information was in conformity with sections 28(2), 29(1) and 30 of the *Act*, as well as whether the information that would be disclosed in response to a police reference check request complies with the disclosure rules in section 32. He found that the collection and use of the information was "for the purposes of law enforcement," as contemplated by sections 28 and 29(1)(g) and that the retention and use of the information was in compliance with section 30.

Under section 32, however, the senior adjudicator concluded that section 6 of Regulation 265/98, promulgated under the Police Services Act, mandates a discretionary approach to the disclosure of the existence of personal information in response to a request for a police reference check. The police appear to have declined to exercise their discretion to not disclose such information and as a result have breached the requirements of section 6 of Regulation 265/98. The proposed disclosure was therefore not in compliance with section 32. On the other hand, if the police reference check program conforms to the requirements of section 6 of the regulation, then section 32(e) would serve as the authority for such disclosure (as noted in section 41(1.2) of the Police Services Act).

Senior Adjudicator Higgins recommended that the police adopt a discretionary process for responding to police reference check requests to conform with the requirements of section 6 of Regulation 265/98. In doing so, the police must bear in mind that this is a discretionary process in which relevant factors must be considered on a case-by-case basis. The senior adjudicator also recommended that the police service exercise its discretion in relation to the specific proposed police reference check request by the appellant.

Privacy

THE PROVINCIAL AND MUNICIPAL *FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACTS* ESTABLISH RULES THAT GOVERN THE COLLECTION, RETENTION, USE, DISCLOSURE, SECURITY, AND DISPOSAL OF PERSONAL INFORMATION HELD BY GOVERNMENT ORGANIZATIONS.

Anyone who believes that his or her privacy has been compromised by a provincial or municipal government organization can file a complaint under the *Acts* with the IPC. In the majority of cases, the IPC attempts to mediate a solution. The IPC may also make formal recommendations to a government organization to amend its practices.

Privacy Complaints

A total of 213 privacy complaints were opened under the two public sector *Acts* in 2007 – an increase of 43 (or 25 per cent) from 2006, when 170 complaints were opened. Of these, 126 (roughly 59 per cent) were filed under the provincial *Act* and 83 (39 per cent) were filed under the municipal *Act*.

There were four non-jurisdictional complaints.

The increase in privacy complaints came primarily as a result of complaints under the provincial *Act*. The total complaints under that *Act* were up by 28 (or just over 28 per cent) from 2006.

Overall, 222 privacy complaints were closed in 2007. This is an increase of 85 from the 137 complaints closed in 2006, representing a 62 per cent jump.

The disclosure of personal information was raised as an issue in 158 (over 66 per cent) of the complaints closed. Another 28 (almost 12 per cent) of the complaints were related to collection, while security was an issue in 20 cases (just over eight per cent). The remaining complaints involved issues including use, retention, notice of collection and consent.

While processing privacy complaints, the IPC continues to emphasize informal resolution. Consistent with this approach, 209 of the 222 privacy complaints closed in 2007 – or about 94 per cent – were closed without the issuance of a formal privacy complaint report or order.

Of the complaints closed, individual members of the public initiated 131 (or 59 per cent) and the Commissioner initiated 91 (41 per cent). This includes investigations into breaches that were self-reported by institutions.

Personal Information Appeals

The provincial and municipal *Acts* provide a right of access to, and correction of, personal information. If you make a request under one of the *Acts* for your personal information and are not satisfied with the response, you can appeal the decision to the IPC.

Personal information appeals can relate to refusal to provide access to your personal information, refusal to correct your personal information, the amount of fees charged, the fact that the organization did not respond within the prescribed 30-day period, or other procedural aspects relating to a request.

When an appeal is received, the IPC first attempts to settle it informally. If all the issues cannot be resolved, the IPC may conduct an inquiry and issue a binding order that may require the government organization to release all or part of the requested information.

Summary of Privacy Complaints – 2007

	2006 Privacy Complaints				2007 Privacy Complaints			
	Provincial	Municipal	Non-jurisdictional	Total	Provincial	Municipal	Non-jurisdictional	Total
Opened	98	72	0	170	126	83	4	213
Closed	82	55	0	137	129	89	4	222

Number of Privacy Complaints Closed 1999 – 2007

Year	Provincial	Municipal	Non-jurisdictional	Total
2007	129	89	4	222
2006	82	55	0	137
2005	52	43	2	97
2004	74	41	11	126
2003	66	60	2	128
2002	54	38	7	99
2001	64	29	6	99
2000	39	41	2	82
1999	40	48	0	88

Privacy Complaints by Type of Resolution

	Provincial		Municipal		Non-jurisdictional		Total	
	No.	%	No.	%	No.	%	No.	%
Informal Resolution	101	77.1	55	63.2	0	0	156	70.3
Withdrawn	8	6.1	13	14.9	0	0	21	9.5
Screened Out	8	6.1	3	3.4	4	100	15	6.8
Settled	5	3.8	6	6.9	0	0	11	4.9
Report	3	2.3	8	9.2	0	0	11	4.9
Abandoned	6	4.6	2	2.3	0	0	8	3.6
Total	**131**	**100**	**87**	**100**	**4**	**100**	**222**	**100**

Source of Complainants

	Provincial		Municipal		Non-jurisdictional		Total	
	No.	%	No.	%	No.	%	No.	%
Individual	57	44.2	70	78.7	4	100	131	59
IPC Commissioner Initiated	72	55.8	19	21.3	0	0	91	41
Total	**129**	**100**	**89**	**100**	**4**	**100**	**222**	**100**

Privacy Complaints by Type of Resolution and Stage Closed

	Intake		Investigation		Total	
	No.	%	No.	%	No.	%
Informal Resolution	154	78.2	0	0	154	69.4
Withdrawn	20	10.2	1	4.0	21	9.5
Screened Out	15	7.6	0	0	15	6.8
Settled	0	0	11	44.0	11	5.0
Report	0	0	11	44.0	11	5.0
Abandoned	8	4.1	0	0	8	3.6
Order Issued	0	0	2	8.0	2	0.9
Total	**197**	**100**	**25**	**100**	**222**	**100**

Issues* in Privacy Complaints

	Provincial		Municipal		Non-jurisdictional		Total	
	No.	%	No.	%	No.	%	No.	%
Disclosure	97	71.3	58	59.8	3	75	158	66.7
Collection	10	7.4	18	18.6	0	0	28	11.8
Security	18	13.2	2	2.1	0	0	20	8.4
Use	2	1.5	6	6.2	0	0	8	3.4
General Privacy Issue	3	2.2	3	3.1	1	25	7	3.0
Retention	2	1.5	3	3.1	0	0	5	2.1
Personal information	1	0.7	1	1.0	0	0	2	0.8
Consent	1	0.7	1	1.0	0	0	2	0.8
Access	0	0	2	2.1	0	0	2	0.8
Accuracy	1	0.7	1	1.0	0	0	2	0.8
Manner of Collection	0	0	1	1.0	0	0	1	0.4
Notice of Collection	0	0	1	1.0	0	0	1	0.4
Disposal	1	0.7	0	0	0	0	1	0.4
Personal Information Bank	0	0	0	0	0	0	0	0
Right of Correction	0	0	0	0	0	0	0	0
Total	**136**	**100**	**97**	**100**	**4**	**100**	**237**	**100**

**The number of issues does not equal the number of complaints closed, as some complaints may involve more than one issue.*

Statistical Overview

In 2007, a total of 957 personal information and general information appeals were submitted to the IPC. This represents an increase of just over seven per cent from 2006, when 893 appeals were received.

Overall, 873 appeals were closed in 2007.

Access or Correction of Personal Information

Appeals Opened

Overall, 386 appeals regarding access or correction of personal information were made to the IPC in 2007 compared to 328 in 2006, an increase of almost 18 per cent. Of these, 185 (almost 48 per cent) were filed under the provincial *Act* and 201 (or about 52 per cent) were filed under the municipal *Act*.

Of the 185 personal information appeals received under the provincial *Act*, 130 (about 70 per cent) involved ministries and 55 (about 30 per cent) involved agencies. The Ministry of Community Safety and Correctional Services was involved in the largest number of personal information appeals (82), followed by the Ministry of the Attorney General (12). The ministries of Labour, Education, Children and Youth Services, and Transportation each had six of their decisions appealed.

Outcome of Issues* in Privacy Complaints

	Provincial		Municipal		Non-jurisdictional		Total	
	No.	%	No.	%	No.	%	No.	%
Resolved – Finding Not Necessary	119	87.5	72	74.2	0	75.8	191	80.6
Act Does Not Apply	12	8.8	13	13.4	4	13.7	29	12.2
Complied in Full	5	3.7	6	6.2	0	6.3	11	4.6
Not Complied	0	0	3	3.1	0	3.2	3	1.3
Order Issued	0	0	2	2.1	0	0	2	0.8
Complied in Part	0	0	1	1.0	0	1.1	1	0.4
Total	**136**	**100**	**97**	**100**	**4**	**100**	**237**	**100**

**The number of issues does not equal the number of complaints closed, as some complaints may involve more than one issue.*

Issues in Personal Information Appeals Opened

	Provincial		Municipal		Total	
	No.	%	No.	%	No.	%
Exemptions Only	111	60.0	131	65.2	242	62.7
Other	23	12.4	16	8.0	39	10.1
Reasonable Search (sole issue)	21	11.4	14	7.0	35	9.1
Exemptions with Other Issues	17	9.2	16	8.0	33	8.5
Deemed Refusal	3	1.6	12	6.0	15	3.9
Correction	2	1.1	4	2.0	6	1.6
Time Extension	4	2.2	0	0	4	1.0
Interim Decision	2	1.1	2	1.0	4	1.0
Third Party	1	0.5	1	0.5	2	0.5
Fee	0	0	2	1.0	2	0.5
Frivolous or Vexatious	0	0	2	1.0	2	0.5
Fee and Fee Waiver	0	0	1	0.5	1	0.3
Fee Waiver	1	0.5	0	0	1	0.3
Inadequate Decision	0	0	0	0	0	0
Failure to Disclose	0	0	0	0	0	0
Transfer	0	0	0	0	0	0
Total	**185**	**100**	**201**	**100**	**386**	**100**

Outcome of Personal Information Appeals Closed by Stage

	Intake		Mediation		Adjudication		Total	
	No.	%	No.	%	No.	%	No.	%
Mediated in Full	0	0	134	97.8	0	0	134	40.7
Ordered	1	1.1	0	0	70	71.4	71	21.6
Withdrawn	47	50.0	2	1.5	8	8.2	57	17.3
Screened Out	34	36.2	0	0	0	0	34	10.3
Other	7	7.4	0	0	9	9.2	16	4.9
Abandoned	5	5.3	1	0.7	9	9.2	15	4.6
No Inquiry	0	0	0	0	2	2.0	2	0.6
Total	**94**	**100**	**137**	**100**	**98**	**100**	**329**	**100**

Outcome of Personal Information Appeals Closed Other Than by Order

	Provincial		Municipal		Total	
	No.	%	No.	%	No.	%
Mediated in Full	59	53.6	75	50.7	134	51.9
Withdrawn	26	23.6	31	20.9	57	22.1
Screened Out	13	11.8	21	14.2	34	13.2
Other	3	2.7	13	8.8	16	6.2
Abandoned	9	8.2	6	4.1	15	5.8
No Inquiry	0	0	2	1.4	2	0.8
Total	**110**	**100**	**148**	**100**	**258**	**100**

Outcome of Personal Information Appeals Closed by Order

	Provincial		Municipal		Total	
Head's Decision	No.	%	No.	%	No.	%
Upheld	16	55.2	24	57.1	40	56.3
Partially Upheld	11	37.9	13	30.1	24	33.8
Other	2	6.9	2	4.8	4	5.6
Not Upheld	0	0	3	7.1	3	4.2
Total	**29**	**100**	**42**	**100**	**71**	**100**

The agencies with the highest number of personal information appeals included the Ontario Human Rights Commission (13), the University of Ottawa (10), and York University and the Archives of Ontario, both with five.

Of the 201 personal information appeals received under the municipal *Act*, 136 (almost 68 per cent) involved police services, 47 (about 23 per cent) involved municipalities, and 13 (6.5 per cent) involved boards of education. Five appeals (2.5 per cent) involved other types of municipal institutions.

Overall, 242 (just under 63 per cent) of appeals were related to the exemptions claimed by institutions in refusing to grant access. In 35 (about nine per cent) of the appeals, the issue was whether the institution had conducted a reasonable search for the records requested.

Another 33 (8.5 per cent) of the personal information appeals related to exemptions plus other issues, and 15 (or just under four per cent) were the result of deemed refusals, where the institution did not respond to the request within the time frame required by the *Act*. The remaining appeals were related to other issues, including fees, time extensions, and interim decisions.

Since personal information appeals, by definition, relate to a request for access and/or correction of one's own personal information, all complainants are categorized as individuals. Overall, just over 70 per cent of appellants represented themselves in these personal information appeals. Lawyers (91) or agents (22) represented appellants in 29.3 per cent of the appeals.

The IPC received $3,340 in application fees for personal information appeals in 2007; these fees were turned over to the Minister of Finance.

Appeals Closed

The IPC closed 329 personal information appeals during 2007, virtually the same number as in 2006. In 2007, 139 (just over 42 per cent) of these appeals concerned provincial institutions, while 190 (almost 58 per cent) concerned municipal institutions.

Of the 329 personal information appeals closed this year, 94 (or almost 29 per cent) were closed at the intake stage, 137 (about 42 per cent) at the mediation stage, and 98 (or about 30 per cent) at the adjudication stage.

Overall, 258 (almost 80 per cent) of personal information appeals were closed without the need to issue a formal order. Orders were issued for the remaining fifth of these appeals.

The IPC issued a total of 71 final orders for personal information appeals – 29 provincial and 42 municipal. Seven interim orders were also issued – one provincial and six municipal.

In appeals closed by order, the decision of the head was upheld slightly more than 56 per cent of the time, and was not upheld or only partially upheld in 38 per cent of cases. Four appeals (5.6 per cent) had other outcomes.

High Profile Privacy Incidents

THE IPC RECEIVED 551 COMPLAINTS IN 2007 UNDER ONTARIO'S THREE PRIVACY ACTS COVERING THE PUBLIC AND HEALTH SECTORS. OVERALL, 599 COMPLAINTS WERE CLOSED. THE FOLLOWING THREE PRIVACY INVESTIGATIONS WERE AMONG THE MOST HIGH PROFILE.

City of Ottawa and Ottawa Police Service, Order MO-2225

In July 2007, the IPC received a complaint from an individual who was concerned with the amount of personal information that second-hand goods stores in the City of Ottawa were required to collect from the people selling them used goods. The complainant also expressed concerns about the stores providing this information to the Ottawa Police Service.

Under a municipal bylaw, used goods stores in Ottawa were required to collect detailed personal information about sellers of used goods, including the seller's name, date of birth, address, their approximate height and weight, and the particulars of two pieces of government-issued identification. The bylaw required that used-goods stores retain this information and make it available for inspection by the police.

The Commissioner launched an investigation. Both the City of Ottawa and the Ottawa Police co-operated fully.

During the course of the investigation, it became evident that many Ottawa used-goods stores were proactively providing the personal information they had collected about sellers to the Ottawa Police. In many cases, this was being facilitated by the use of computer software provided by a private company. The software enabled the Ottawa Police to remotely access transaction details, including personally identifying information about sellers.

There had been a court ruling a few months earlier about a very similar case. In Cash Converters Canada Inc. v. Oshawa (City) (Cash Converters), the Ontario Court of Appeal dealt with a challenge to a similar bylaw and information-collection regime that was in place in the City of Oshawa. In its decision, the Court considered the IPC's past decisions relating to the collection of personal information under section 28(2) of the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*) and ruled that the impugned provisions of the bylaw conflicted with the *Act*. As a result, the Court made a significant ruling, stating that those provisions of the Oshawa bylaw were "of no force or effect."

In dealing with the privacy complaint involving the City of Ottawa and the Ottawa Police, the Commissioner carefully considered information provided by both institutions relating to the purpose and history of the bylaw. Based on a review of the material provided, as well as the precedent established by the Court of Appeal in Cash Converters, the Commissioner found that both the collection of personal information required under the municipal bylaw and the eventual disclosure and collection of this information by the Ottawa Police contravened section 28(2) of the *Act*.

The Commissioner issued an order under section 46(b) of the *Act* requiring the cessation of the collection of personal information in contravention of the *Act* and the destruction of personal information that had been collected in the past. The order applied to both the Ottawa Police's collection of personal information and the collection of personal information by the used-goods stores pursuant to the bylaw.

This was the first order ever issued in this area that exercised our "cease collection and destroy records" authority under section 46(b).

In the order, the Commissioner acknowledged that used-goods stores may need to collect some contact information from sellers of used goods, but that this information should only be collected for the store's own legal or business purposes, and not for a different purpose under a municipal bylaw. The order also made it clear that personal information about sellers should no longer be proactively disclosed to the Ottawa Police.

Order HO-004 The Hospital for Sick Children

On January 15, 2007, the IPC was contacted about a stolen laptop computer belonging to the Hospital for Sick Children (SickKids). The laptop contained the personal health information of current and former SickKids patients.

The IPC immediately commenced an investigation of this incident pursuant to the *Personal Health Information Protection Act* (the *Act*).

On January 4, 2007, a physician at SickKids, who was both a clinician and a researcher, had left the hospital with one of its laptop computers, intending to take it home to analyse research data that was stored on it. The physician did not, however, go directly home. Instead, he parked his minivan in a parking lot in downtown Toronto. When he returned he found that his minivan had been broken into and the laptop had been stolen. He reported the theft to the police and to SickKids, which, in turn, conducted an internal investigation and notified the IPC of the incident.

SickKids advised the IPC that the data on the laptop consisted of Excel spreadsheets containing the personal health information of approximately 2,900 current and former SickKids patients involved in five prospective and five retrospective research studies.

The amount of information pertaining to each patient varied, but in all cases, included identifiable personal health information (PHI) including the patient's name, SickKids hospital number and some information relating to the patient's medical condition. In some cases, very sensitive information was also included, such as answers provided in interviews and questionnaires relating to morbidity and mortality details, perceptions of quality of life, drug therapy, and HIV status.

All of the data stored on the laptop was also saved on SickKids' main server. The only laptop security used was an eight-character alphanumeric login password. No encryption of any data had been enabled at either the file or disk level.

At the time of the incident, remote encrypted access to PHI in shared folders was available to researchers through standard commercial software via a Virtual Private Network, and to clinicians for access to clinical applications through commercial software called CitrixTM. SickKids acknowledged that the researcher could have accessed this data remotely, which would have eliminated the need to remove it from the hospital on the laptop computer. SickKids also acknowledged that, in this particular case, the research data did not need to be accessed in identifiable form.

After the incident, SickKids undertook the process of notifying the affected individuals of the theft of the laptop.

On March 7, 2007, following the completion of the investigation, the Commissioner issued her fourth order (HO-004) under the *Act*.

The Commissioner found that many of the requirements under the *Act* relating to the retention and security of PHI and its use in a research setting were absent from SickKids' current policies across many departments, and that SickKids did not ensure that the PHI in its custody and control was retained in a secure manner.

Based on her findings, the Commissioner ordered SickKids to:

- develop or revise and implement policies and procedures to ensure that any PHI removed from the hospital in electronic form is either de-identified or encrypted;
- develop a policy relating to the use of secure remote access;
- develop a privacy breach protocol;
- review and revise its research protocols to ensure compliance with the *Act*; and
- educate and train staff regarding its new policies.

The Commissioner emphasized that health information custodians should avoid storing identifiable PHI on mobile computing devices. Where PHI must be stored on such devices, only the minimal amount of information necessary

should be stored and for the minimal amount of time necessary to complete the work. The Commissioner also stressed that any PHI contained on a mobile computing device must be either de-identified or encrypted. In either of these instances, she would not consider the theft or loss of a device to be a loss or theft of PHI.

When the order was released, the IPC, to assist health-care providers, also issued a fact sheet, *Encrypting Personal Health Information on Mobile Devices*, and a brochure, *Safeguarding Privacy in a Mobile Workplace*, which provide direction on encryption and safeguarding privacy on mobile devices.

Order HO-005 Larch Street Methadone Clinic

On April 30, 2007, the IPC was contacted by a reporter who advised that a video image of a patient attending a Sudbury methadone clinic had appeared on a wireless mobile rear-assist parking device (a "back-up camera" designed to improve visibility when a vehicle is in reverse), in a car parked near the clinic. The IPC immediately commenced an investigation pursuant to the *Personal Health Information Protection Act*.

The reporter, who was from the Canadian Broadcasting Corporation (CBC), advised the IPC that she had been initially notified of the situation by an individual who, much to his surprise, had seen images from a washroom on his vehicle's back-up camera.

The reporter enlisted a private investigator to determine if this could be true. The reporter and the investigator parked their car in same parking lot where the original incident occurred. From there, they saw an image of the washroom in their back-up camera screen. While they were trying to figure out which building the image might be coming from, a woman entered the washroom and used the facilities.

Shortly thereafter, the woman viewed on the screen exited a nearby building. They approached the woman, who indicated that the facility she had just attended was a methadone clinic, and that she was aware of the presence of a surveillance camera in the washroom. She indicated that patients of the clinic are monitored while providing urine samples to ensure that the samples are not tampered with. In addition, she advised the reporter that her written consent had been sought and provided to the clinic for it to engage in this practice, but not, much to her surprise, having the images broadcast outside of the clinic.

Upon being notified of the incident by the CBC, the IPC immediately contacted the clinic. The IPC advised the clinic of the two incidents and asked it to immediately turn off the camera (which it did) and to contact its security firm to ensure that this type of incident could not occur again. The clinic contacted its security firm and a technician was dispatched that day.

The technician advised the clinic that its surveillance cameras operated on wireless technology and that, as a result, the images in the camera could be viewed on any other wireless device using the same frequency. The clinic had not been informed of this, and was also unaware of the implications of having a wireless system, namely, that the images could be intercepted.

The clinic advised the IPC that its surveillance system did not record the images captured by the cameras, as no recording devices were connected to the system. The system was designed so that the images could only be monitored in real time by clinic staff in the nurse's observation station. In addition, the system was not connected to a computer or the Internet.

After the incident, the clinic worked with the IPC to post a notice on the premises regarding the incident. The wireless system was replaced with a wired one.

Following the completion of the investigation, the Commissioner issued her fifth order (HO-005) under the *Act* on June 7, 2007. The Commissioner found that the video image constituted a record and met the definition of personal health information under the *Act*, and that, had the clinic conducted regular privacy and security reviews, it was likely that it would have become aware of the increased risks posed by emerging wireless technologies and taken steps to modify its monitoring system.

Based on her findings, the Commissioner ordered the clinic to conduct an annual security and privacy review of its personal health handling systems and procedures to ensure continued compliance with the *Act*.

The Commissioner emphasized that, given the significant threat to privacy that wireless technology poses, health information custodians who use video surveillance should either use a wired system, which inherently prevents interception, or a wireless one with appropriate protections, such as strong encryption, and annual reviews, to preclude unauthorized access. In addition, health information custodians should regularly review their privacy and security policies to ensure that the risks associated with the use of technology are minimized.

When the order was issued, the IPC also released two fact sheets, *Wireless Communication Technologies: Video Surveillance Systems* and *Wireless Communication Technologies: Safeguarding Privacy & Security*, which provide valuable advice on safeguarding privacy in a wireless world.

The *Personal Health Information Protection Act (PHIPA)*

2007 WAS A BUSY YEAR ON THE HEALTH PRIVACY FRONT. PUBLIC AWARENESS OF THE *PERSONAL HEALTH INFORMATION PROTECTION ACT (PHIPA)* AND OF THE COMPLAINTS PROCESS AVAILABLE THROUGH THE IPC CONTINUED TO GROW AS THE LEGISLATION MARKED ITS THIRD ANNIVERSARY.

In resolving complaints, the IPC maintained its focus on mediation and alternative dispute resolution methods. Consequently, only two health orders were issued in 2007, both as a result of privacy breaches stemming from the use of information and communication technology in health care.

Over the course of this past year, the IPC continued to work with health information custodians to help them refine their information practices, commenting on draft policies and procedures and issuing detailed guidance in response to recurring privacy issues. We also distributed thousands of copies of our more than 20 publications dedicated specifically to *PHIPA* at major health conferences.

All of the IPC publications cited in this chapter are available on the IPC's website, www.ipc.on.ca.

Three-Year Review

The IPC launched an internal review of *PHIPA* late in 2007, after the end of the *Act's* third year in force (which occurred November 1, 2007).

As well as the IPC's review, the legislation requires a committee of the Legislative Assembly to conduct a comprehensive review of *PHIPA's* first three years.

Recently, Commissioner Cavoukian stressed the importance of the legislation. "As the person responsible for overseeing *PHIPA* over the past three years, I can attest to the fact that the legislation was well-crafted and is operating smoothly. It was designed to have a minimal impact on the delivery of healthcare services by allowing health information custodians to rely on implied consent within the circle of care, but requiring express consent outside of this trusted circle."

Health Privacy Day – The Privacy Prognosis in an Era of New Health Information Technology

September 24 was *Health Privacy Day* in Ontario.

To mark the occasion, the IPC sponsored an international conference, *The Privacy Prognosis in an Era of New Health Information Technology*. The conference was devoted to privacy issues surrounding emerging health information technologies. It complemented the International Privacy and Data Protection Commissioners' Conference, which was held later the same week in Montreal.

The IPC conference was well attended by a broad range of participants including Privacy and Data Protection Commissioners from around the world, health policy decision-makers and strategists, health regulatory bodies, privacy advocates, privacy consultants, chief privacy officers, health information technology developers, academics, and students.

Follow-up on the IPC Review of Smart Systems for Health Agency

In last year's Annual Report, the IPC reported on its review of the Smart Systems for Health Agency (SSHA), which supplies electronic goods and services to health information custodians as defined under *PHIPA*. The review was conducted in accordance with section 6.1 of Ontario Regulation 329/04, which requires SSHA to put in place administrative, technical and physical safeguards, and practices and procedures reviewed by the IPC.

In its report, the IPC made 82 recommendations to help ensure a high level of data protection as Ontario transforms the delivery of health-care services by implementing new information and communications technologies. The report was published in March 2007.

In light of its findings, the IPC later in 2007 expressed concerns about the government's proposal to move Ontario's Electronic Master Patient Index (EMPI) from Cancer Care Ontario (CCO) to SSHA in the fall of 2007.

The EMPI is a registry of all individuals who receive health care in the province. It supports integration of health services by enabling an individual's personal health information to be consistently linked across the health sector. When fully implemented, the EMPI will play a central role in all e-health initiatives in Ontario.

The IPC asked for, and received, copies of two privacy impact assessments conducted on behalf of SSHA – one specific to the EMPI system itself and the other related to the transitioning of the EMPI from the CCO to SSHA.

The IPC also commissioned an independent consultant, David Flaherty, former B.C. Information and Privacy Commissioner, to assess the extent to which SSHA had implemented the IPC's recommendations prior to the transition. The consultant was also asked to examine whether SSHA would have adequate safeguards in place with regard to the EMPI during and after the transition.

The consultant's report was published on the IPC website in October 2007. Although he raised concerns about SSHA's failure to make its privacy and security policies and procedures available to the public, he concluded that SSHA had made demonstrable progress towards full compliance with the IPC's recommendations. He further concluded that there were no privacy and security concerns with the transfer of the EMPI from CCO to SSHA, recognizing that control of the EMPI would continue to rest with the Ministry of Health and Long-Term Care.

Following the review, the Commissioner wrote a letter to the SSHA. In it, she indicated that, provided that the issue of transparency with respect to SSHA's information practices could be resolved in a timely way, she was satisfied that the privacy and security safeguards were sufficient to support the transfer of the operation of the EMPI from CCO to SSHA.

The transfer officially took place January 1, 2008.

Reviews of Prescribed Entities and Persons

In 2005, the IPC reviewed and approved the information practices and procedures of four prescribed entities and four prescribed persons who compile or maintain registries of personal health information.

When the IPC reviews and approves the information practices of prescribed entities and prescribed persons, it issues reports to the organizations that include a number of recommendations to enhance the privacy and security of the personal health information collected, used and disclosed by the entities and persons. These reports are available on the IPC website.

In 2006, the Critical Care Information System was added as a registry, with Hamilton Health Sciences Corporation being prescribed as the "person" that compiles or maintains the registry. In 2007, Cancer Care Ontario was also prescribed as the person that compiles or maintains the Colorectal Cancer Screening Registry. The IPC will be reviewing the information practices and procedures of both these organizations shortly.

In the meantime, the IPC met in 2007 with each of the organizations whose practices had been reviewed in 2005 to follow up on the status of their compliance with the IPC's recommendations. Each of the IPC's recommendations had been implemented or were in the process of being implemented.

Preventing Abandonment of Records of Personal Health Information

Changes in the practices of health information custodians may occur in a variety of circumstances, including death, bankruptcy, retirement or relocation. In some cases, these changes result in records of personal health information being left in inappropriate places.

A failure to adequately address privacy and security issues with respect to the treatment of personal health information in the event of a change in practice may lead to privacy breaches,

including the unauthorized disclosure and the denial of the individual's right to access and correct records. It may also jeopardize the continuity of care to the individual.

This year, the IPC issued a fact sheet, *How to Avoid Abandoned Records: Guidelines on the Treatment of Personal Health Information, in the Event of a Change in Practice*, to help ensure personal health information is handled in accordance with the privacy and security requirements of *PHIPA*.

The *Guidelines* provide information about correctly identifying health information custodians, what their obligations are, and best practices. They encourage custodians to think proactively about how they will continue to meet their obligations under *PHIPA* in the event of a change in practice by being aware of privacy-protective record-keeping practices, clearly identifying the custodian (especially in group practices), and addressing privacy safeguards and record management continuity.

To accompany the *Guidelines*, the IPC also issued a *Checklist for Health Information Custodians in the Event of a Planned or Unforeseen Change in Practice*. It provides a quick reference guide to help ensure that, in the event of a change in practice, health information custodians:

- correctly identify who the health information custodian is;
- retain records in a secure manner;
- transfer records in a secure manner;
- dispose of records in a secure manner;
- notify patients about the change in practice;
- ensure that an appropriate person provides the notice to patients; and
- provide sufficient detail in the notice to patients.

The *Checklist* also provides a list of steps health information custodians should take to safeguard personal health information prior to a change in practice.

Preventing Privacy Breaches When Using Information and Communication Technology

PHIPA requires health information custodians to take steps that are reasonable in the circumstances to ensure that personal health information in their custody or control is protected against theft, loss and unauthorized use or disclosure, and to ensure that records containing personal health information are protected against unauthorized copying, modification or disposal.

In January 2007, Commissioner Cavoukian issued her fourth Order under *PHIPA* after a laptop computer containing a large number of records of personal health information from a hospital was stolen from a parked vehicle. (Please see the chapter entitled *High Profile Privacy Incidents* for a more detailed discussion about this incident.)

In the order, the Commissioner sent a strong message to health information custodians that it is not reasonable to store personal health information on mobile devices, such as laptop computers, personal digital assistants or flash drives, unless steps are taken to protect it. Further, she stressed that passwords, which can be readily circumvented, are not sufficient protection.

Because of the high incidence of loss or theft of mobile devices, the Commissioner stressed that health information custodians need to ensure that any personal health information that is stored on them is encrypted. To the extent that personal health information on a mobile computing device has been effectively encrypted, and therefore inaccessible, the Commissioner advised that the loss or theft of the device would not be considered a loss or theft of personal health information.

To assist health information custodians, the IPC issued a fact sheet entitled *Encrypting Personal Health Information on Mobile Devices*.

The IPC also issued a brochure, *Safeguarding Privacy in a Mobile Workplace*, to provide guidance for individuals who take their work "on the road." The brochure outlines a number of best practices for protecting mobile devices and any personal information that they may contain.

Wireless Technologies

In June 2007, the Commissioner issued her fifth Order under *PHIPA* after video surveillance images of a patient using a washroom at a methadone clinic appeared on a monitor in a car that had a wireless mobile rear-assist parking device ("back-up camera"). The incident is outlined in detail in the chapter *High Profile Privacy Incidents*.

Wireless devices transmit information over radio waves that are broadcast in all directions from the point of transmission, making the information accessible to any receiver within the devices' range. Since there are a limited number of radio frequency bands available for transmitting information, the risk of inadvertent interception of information that is being transmitted from a wireless device is relatively high.

In her order, the Commissioner sent an urgent message to health information custodians who opt to use wireless technology in their practices. She warned that, given the significant threat to privacy that wireless technology poses, health information custodians who use video surveillance in their practices should either use a wired system, which inherently prevents such interception, or a wireless one with appropriate measures, such as strong encryption, to preclude unauthorized interception. She also reminded custodians to regularly review their privacy and security policies to minimize the significant risk to privacy posed by new technologies.

To assist health information custodians in safeguarding privacy and security with wireless communication technologies, the IPC issued two fact sheets. The first, *Wireless Communication Technologies: Video Surveillance Systems*, provides guidance for protecting privacy when using wireless video surveillance systems for transmitting personal health information. The second, *Wireless Communication Technologies: Safeguarding Privacy & Security*, provides general guidance on the protection of privacy when using any wireless communication technology.

Determinations

Whenever records of personal health information must be inspected without the individual's consent in the course of a review, the Commissioner must first determine that it is reasonably necessary to do so and that the public interest in carrying out the review justifies dispensing with consent in the circumstances. The Commissioner must also provide a written statement to the person who has custody or control of the record, setting out her determination, reasons, and any restrictions and conditions the Commissioner has specified.

In 2007, the Commissioner made one such determination as part of her investigation into reports that records of personal health information were abandoned when a dental clinic closed without notice to patients.

The investigation was launched after the Royal College of Dental Surgeons of Ontario wrote to the IPC stating that it had been contacted by a number of patients of a dentist in the Ottawa area who reported that the dental clinic had closed and asked for assistance in gaining access to their dental records.

After repeated attempts to contact the owner of the clinic by the College, repeated notices to the owner by the Commissioner and a visit to the abandoned dental clinic by an IPC staff member, the Commissioner decided to exercise her powers of seizure under *PHIPA* and entered the clinic to take possession of the records of personal health information. The College agreed to take custody of the records, to ensure secure storage and to facilitate the patients' right of access to the records.

In this case, it was not possible for the Commissioner to obtain the patients' consent prior to retrieving the records of personal health information, since the identities of the patients were unknown to the Commissioner. The Commissioner determined that it was necessary to dispense with consent in the circumstances.

Statistical Review

Statistics related to requests for access to personal health information or privacy complaints filed under *PHIPA* are collected in two different ways for this Annual Report: internally and externally.

The internal collection is from the IPC's own records, showing the number and nature of all privacy complaints filed with the IPC in 2007 under *PHIPA*. These are reported in the *Privacy Complaints* section of this chapter.

The external collection is through the reports filed by organizations that report to the IPC about *PHIPA*-related matters.

External statistical reporting requirements under *PHIPA* do not provide for a comprehensive picture. All government organizations covered under the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act* are required to file a detailed statistical report to the IPC each year. *PHIPA* covers much more than government organizations, however. Only government organizations that are also health information custodians or that employ one or more health information custodians (such as

doctors, nurses, or ambulance services) are required to report *PHIPA*-related information annually. A few custodians, such as some hospitals, are reporting voluntarily.

A brief review of access requests filed with health information custodians, based on the available external statistics, is provided in the section of this chapter entitled *Personal Information Requests*.

Percentage figures given here have been rounded off and may not add up to 100.

Privacy Complaints

Complaints Opened

There were 338 complaint files opened under *PHIPA* by the IPC in 2007, an increase of just over 25 per cent from the 269 complaints opened in 2006 and almost twice the number (177) opened in 2005, the legislation's first full year.[1]

Public hospitals accounted for 147 of the 338 complaints opened, or about 43 per cent, a much higher percentage than in either of the previous two years (24.5 per cent in 2006, 26.6 per cent in 2005).

There were 47 complaints opened involving doctors (almost 14 per cent), 26 involving clinics (almost eight per cent), 18 involving community or mental health centres, programs or services (about five per cent), and about three per cent each for the Ministry of Health and Long-Term Care and community care access centres. The remaining complaints involved other types of health information custodians or agents.

Overall, 111 (almost 33 per cent) of the complaints opened in 2007 related to access to and/or correction of personal health information. The remaining 227 dealt with the collection, use or disclosure of personal health information. Of these, 139 complaints were self-reported by health information custodians (about 41 per cent of the total number of complaints), while 62 were filed by individuals (about 18 per cent). Another 26 (almost eight per cent) were initiated by the Commissioner.

Complaints Closed

The IPC closed 338 complaints in 2007, an increase of about 21 per cent over the 279 complaints closed in 2006.

Of the complaints closed, 120 (almost 36 per cent) dealt with access to and/or correction of personal health information, while the other 218 dealt with collection, use or disclosure. Of the second type, 139 (about 41 per cent of the overall number of complaints closed) arose from privacy breaches self-reported by health custodians. Commissioner Cavoukian actively encourages this kind of self-reporting.

The remaining privacy complaints related to collection, use or disclosure that were closed in 2007 included 51 (about 15 per cent) filed by individuals and 28 (about eight per cent) initiated by the Commissioner.

Of the 120 complaints closed that were related to access to and/or correction of personal health information, 54 (45 per cent of this category) were the result of deemed refusals, where a health information custodian fails to respond to the request within the statutory time frame.

Fees were the issue in 14 (almost 12 per cent) of the complaints, and 11 (just over nine per cent) were about whether the health information custodian had conducted a reasonable search for the records requested. There were eight complaints related to the correction of personal health information. The exemptions applied to deny access to personal health information were the subject of five complaints. The remaining 28 complaints involved other issues.

As much as possible, the IPC prefers to resolve complaints either informally or through mediation. All 120 complaints dealing with access to and/or correction of personal health information were resolved without the IPC needing to issue an order. Of these, 84 (70 per cent) were closed informally at the intake stage, 28 (about 23 per cent) were closed during the mediation stage, and eight (almost seven per cent) were closed during the adjudication stage without an order having to be issued.

[1] *PHIPA came into effect on November 1, 2004.*

PHIPA Complaints Opened 2007

Custodians, Agents and Others	Access/ Correction	Collection/Use/Disclosure: Initiated by Individual	Collection/Use/Disclosure: Self-reported Breach	Collection/Use/Disclosure: IPC-Initiated	Total	%
Public Hospital	40	25	76	6	147	(43.5)
Doctor	26	11	5	5	47	(13.9)
Clinic	10	3	7	6	26	(7.7)
Others (including Agents)	6	12	8	2	28	(8.3)
Community or Mental Health Centre, Program or Service	4	2	11	1	18	(5.3)
Ministry of Health	6	2	3	0	11	(3.3)
Community Care Access Centre	1	0	9	0	10	(3.0)
Agent	7	0	0	2	9	(2.7)
Nursing Home	5	0	1	0	6	(1.8)
Laboratory	1	1	3	1	6	(1.8)
Pharmacy	1	0	3	2	6	(1.8)
Other Health Care Professional	1	1	4	0	6	(1.8)
Other Prescribed Person	0	0	4	0	4	(1.2)
Independent Health Facility	0	1	2	0	3	(0.9)
Dentist	1	1	0	1	3	(0.9)
Drugless Practitioner	1	1	0	0	2	(0.6)
Home or Joint Home (Aged or Rest Home)	1	1	0	0	2	(0.6)
Nurse	0	1	1	0	2	(0.6)
Social Worker	0	0	2	0	2	(0.6)
Total	**111** (32.8%)	**62** (18.3%)	**139** (41.1%)	**26** (7.7%)	**338** (100%)	

Similarly, the overwhelming majority of the collection, use or disclosure complaints closed were resolved informally or through mediation. Of the 218 privacy complaints in this category, the IPC needed to resolve only two through orders.

Of the 51 initiated by individual complainants, 42 (about 82 per cent) were closed during the intake stage and nine (almost 18 per cent) were closed during the mediation stage.

Of the 28 complaints dealing with the collection, use and disclosure of personal health information that the Commissioner initiated, 20 (just over 71 per cent) were closed at the intake stage and seven (25 per cent) at the mediation stage, with one complaint going to adjudication and being closed with an order.

Of the 139 complaints that involved self-reported privacy breaches by health information custodians, 130 (almost 94 per cent) were closed at the intake stage, eight (about six per cent) at the mediation stage and one was closed with an order.

Personal Health Information Requests

Government institutions reported that a total of 2,839 requests from individuals seeking access to/or correction of their personal health information were completed in 2007. This represents an increase of nearly 44 per cent from 2006.

Overall, 2,450 requests, representing most of the increase, were reported by the Ministry of Health and Long-Term Care. The ministry's requests were up 42 per cent from the 1,772 received in 2006. The ministry's 30-day compliance rate was also up. Over 99 per cent of requests were completed in the 30-day period (up from 98.1 per cent the year before). Full access was provided in 2,402 cases – 98 per cent of requests, up from 96.2 per cent in 2006.

The ministry charged fees for 79 requests (about three per cent of cases), and collected $1,935.50 for an average fee of $24.50 per request where a fee was charged. In four cases, records were not accessed following a fee estimate.

Other types of health information custodians reported the remaining 389 requests. Medical Officers of Health/Boards of Health handled 204 of them, and completed 194 or about 95 per cent within the 30-day compliance period. The Brant County Health Unit had the most requests (92), and completed all of them within 30 days. For this category of health information custodian, full access to the requested material was provided in just over 85.5 per cent of the requests. They charged fees for 46 of the 204 requests and collected $2,384.10 for an average of $51.83 for each request that was subject to fees.

Ambulance services completed 86 requests. They charged fees for 50 of the 86 requests, collecting an average of $55.06. Peel Region Paramedic Services had the highest number of requests (26).

Health-care providers working for school boards, and homes for the aged and nursing homes accounted for most of the remaining requests.

Judicial Reviews

THE ONTARIO COURTS ISSUED A NUMBER OF IMPORTANT DECISIONS IN 2007, INCLUDING ONE APPLYING THE CANADIAN CHARTER OF RIGHTS AND FREEDOMS WHICH EXPANDED THE CIRCUMSTANCES UNDER WHICH THE PUBLIC INTEREST MAY OVERRIDE THE APPLICATION OF EXEMPTIONS UNDER THE *FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT (FIPPA)*.

In effect, the Court amended *FIPPA* in a way that the IPC had been advocating since 1994 but did not have the authority to change. Section 23 of *FIPPA* states that where a "compelling public interest" in disclosure "clearly outweighs" the purpose of certain exemptions from the right of access, those exemptions do not apply. The Court of Appeal ruled that the exemptions for law enforcement (section 14) and solicitor-client privilege (section 19) must now be added to the list of exemptions subject to the section 23 override.

The Criminal Lawyers' Association (CLA) had sought access to records relating to allegations of police and Crown misconduct in a murder case. The IPC upheld the Ministry of Public Safety and Security's decision that the records were exempt under the law enforcement and solicitor-client privilege exemptions. In addition, the IPC found that although there was a compelling public interest in disclosure, the records could not be disclosed since section 23 did not apply to the section 14 and 19 exemptions.

In a 2-to-1 decision, the Court of Appeal held that the CLA was attempting to exercise its freedom of expression under section 2(b) of the Charter by commenting on the alleged misconduct. The Court stated that, as a result of being denied access to the records, the CLA was unable to comment in any substantial way.

The majority held that the Legislature's primary purpose in enacting FIPPA was to assist in the exercise of expression and that any limits on this scheme amounted to a restriction on expression. They found that the exclusion of sections 14 and 19 from section 23 had the effect of infringing on expression, and that the infringement could not be justified under section 1 of the Charter. As a result, the majority ruled that sections 14 and 19 must be "read in" to section 23.

As a result of the Court of Appeal's decision, the IPC now has the ability to decide independently whether records subject to the law enforcement and solicitor-client privilege exemptions should be disclosed in the public interest.

The Supreme Court of Canada has granted the ministry's application for leave to appeal the Court of Appeal's decision. This appeal is tentatively scheduled to be heard by the Supreme Court in the fall of 2008.

In another important decision, the Divisional Court affirmed the IPC's long-standing approach to the disclosure of information about legal fees under *FIPPA*. The case involved two decisions in which the IPC found that total dollar figures on invoices for legal services rendered to the government could not be withheld under the section 19 solicitor-client privilege exemption

In the first case, the fees involved were for legal services provided to two ministries in defending lawsuits regarding the province's provision of services to children with autism. The second case involved fees for legal services rendered in a series of appeals with respect to funding for medical testing for a rare form of eye cancer.

The Court agreed with the IPC's interpretation that while legal accounts are subject to a presumption of privilege, that presumption may be rebutted where the disclosure of the information would not violate the confidentiality of the solicitor-client relationship by revealing privileged communications. Further, the Court held that the IPC did not err in finding that in both cases, the presumption of privilege was rebutted, particularly since the requesters asked only for the total amount of fees and did not seek any account details that would permit them to infer privileged information.

In yet another important 2007 decision, the Divisional Court considered requests by the Toronto Star for access to police electronic databases. The Court ruled that the police were not required to provide access by replacing individual names with randomly generated, unique numbers. The requester specifically stated that he did not want access to any information that would identify individuals.

The IPC found that the Toronto Police Services Board was required to provide the requester with the type of access he requested, since producing the record would not "unreasonably interfere with the operations of" the police. The Court found that the IPC erred in failing to consider whether the record was capable of being produced by means "normally used by the institution" under the section 2(1) definition of "record" in the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*.

The Ontario Court of Appeal has granted the IPC and the Toronto Star leave to appeal the Divisional Court's decision.

In a fourth case, involving access to information about firearms used in crimes, the Divisional Court ruled that the term "law enforcement matter" is not limited to a specific, ongoing investigation or proceeding.

The Toronto Star made a request to the Ministry of Community Safety and Correctional Services for access to information held by the Provincial Weapons Enforcement Unit relating to trace information about weapons found in Canada but not registered in Canada. The ministry denied access to the information based on various parts of the section 14 "law enforcement" exemption in *FIPPA*.

The IPC upheld the ministry's decision in part and ordered the ministry to disclose certain limited information that did not qualify for exemption under section 14. Both the Toronto Star and the ministry applied for judicial review of the IPC's order.

The Court agreed with the IPC's finding that to support the application of the section 14 exemption, the ministry must provide "detailed and convincing evidence" to establish a reasonable expectation of harm to the specific law enforcement interests. The Court upheld the IPC's decision that some of the information qualified for exemption under section 14(1)(g) (intelligence information), and dismissed the Toronto Star's application.

With respect to the ministry's application, the Court held that the IPC reasonably concluded that sections 14(1)(c) (investigative techniques) and (l) (facilitate the commission of an unlawful act) did not apply. However, the Court ruled that the IPC erred in narrowly interpreting the term "law enforcement matter" to encompass only specific and ongoing investigations. In any event, the Court stated that in these circumstances, the information at issue is both "specific" and "ongoing."

In a fifth case considered by the courts in 2007, the Divisional Court upheld the IPC's application of the personal privacy exemption. The case involved a letter from an individual to a municipality about a proposed property development. The individual, a member of the public, wrote to the municipality voicing her concerns about the impact of the proposal.

The property development company sought access to the letter, and the Town of Innisfil denied access on the basis of section 14 of *MFIPPA*. The IPC upheld the town's refusal, holding that the Planning Act did not expressly authorize the disclosure, and that the factors in section 14(2) in favour of confidentiality outweighed the factors in favour of disclosure. The IPC concluded that disclosure of the letter would constitute an unjustified invasion of the individual's personal privacy under section 14.

On judicial review, the Court accepted the IPC's submission that while the record may be permitted or required to be disclosed to the public under the Planning Act, the record may still qualify for exemption under *MFIPPA*. The Court

found the IPC's interpretation and application of the section 14 exemption to be reasonable and, therefore, dismissed the development company's application.

This decision confirms the IPC's long-standing view that *FIPPA* and *MFIPPA* are not intended to operate as a complete code for the disclosure of information in the administrative justice system in Ontario.

Finally, in a sixth case decided in 2007, the Divisional Court upheld the IPC's interpretation and application of the third party commercial information exemption at section 17 of *FIPPA*.

The requester sought access to records relating to the request for proposal process initiated by the Ministry of Health and Long-Term Care for the provision of CT and/or MRI services at independent health facilities to be located in several Ontario communities. The ministry denied access to the records, mainly on the basis of section 17.

The IPC held that the records did not qualify for exemption, since the ministry and the two affected parties (who had submitted the proposals in question) had failed to provide detailed and convincing evidence to establish that disclosure could reasonably be expected to result in any of the harms listed under section 17.

The two affected parties brought judicial review applications to the Divisional Court. The Court held that the Commissioner's conclusions on the harms under section 17 were reasonable and consistent with prior IPC decisions.

2007 Judicial Review Statistics

New Judicial Review applications received in 2007:

Launched by:	
Institutions[1]	8
Requesters	0
Affected Parties[2]	2
Total	**10**

Outstanding Judicial Reviews as of December 31, 2007:

Launched by:	
Institutions	12
Requesters	0
Institution and Other Party	4
Affected Parties	7
Total	**23**

Judicial Reviews Closed/Heard in 2007:

Abandoned (Order Stands)[1]	2
Heard but Not Closed (decision pending)[4]	2
Matter Remitted Back to IPC	0
IPC Order/Decision Upheld[5]	4
IPC Order Not Upheld (appeal pending)[6]	2
IPC Order Upheld in Part[7]	1
Dismissed for Delay (Order stands)[8]	1
Total	**12**

[1] *MO-2199, PO-2494 & PO-2532-R, PO-2498, PO-2405 & PO-2538-R, PO-2598, PO-2601-I*

[2] *Reconsideration decision re: PO-2491, PO-2620*

[4] *PO-2367, PO-2390*

[4] *PO-1905 (Div.Ct.), MO-1966 (C.A.)*

[5] *MO-1936, PO-2367, PO-2484, PO-2548*

[6] *MO-1989 (IPC's/Requester's appeals to C.A. pending), PO-1779 (Ministry's appeal to S.C.C. pending)*

[7] *PO-2455*

[8] *MO-1929*

Information About the IPC

REACHING OUT

The IPC's extensive outreach program helps to increase awareness of Ontario's access and privacy laws and related issues.

The program has six key elements:

- Targeted outreach through the *Right to Know* and *Reaching Out to Ontario* programs;
- A school-based initiative entitled *What Students Need to Know about Freedom of Information and Protection of Privacy*;
- A publications program;
- A public speaking program;
- An aggressive proactive media relations program; and
- A content-rich website.

Targeted Outreach

There are several specifically targeted initiatives within the corporate outreach program, including the *Right to Know* and the *Reaching Out to Ontario* initiatives.

Under the *Right to Know* program, the IPC organized two special events in 2007. The first was a *Right to Know Blitz Day* on September 28, which is *International Right to Know Day*. To mark the occasion, tables were set up at four Toronto-area malls. IPC staff handed out publications and answered questions from the public.

Then, on October 31, the IPC co-sponsored a *Right to Know Luncheon* with the Toronto Regional Group of the Institute of Public Administration of Canada. A blue-ribbon panel explored a variety of issues related to Ontarians' right to know and debated what is working and what is not in government openness and transparency. The panel was moderated by Commissioner Cavoukian and included Ombudsman André Marin, Auditor General Jim McCarter, and Conflict of Interest Commissioner Justice Sidney B. Linden.

This past year, the IPC also organized several special events that focused on health privacy. On September 24, which Commissioner Cavoukian designated as *Health Privacy Day*, the IPC hosted a conference, *The Privacy Prognosis in an Era of New Health Information Technology*. The conference was a precursor to the annual International Privacy and Data Protection Commissioners conference, which was held in Montreal, and was attended by privacy and data protection experts from around the world.

School Program

The IPC's popular school program, *What Students Need to Know about Freedom of Information and Protection of Privacy*, offers free teachers' kits tailored to three levels: the Grade 5 social studies curriculum (where students first study government), the Grade 10 civics curriculum, and Grade 11 and 12 history and law courses. The program is supported by IPC staff presentations to a number of Grade 5 classes every school year.

All three teachers' guides were developed by the IPC with the aid of curriculum professionals and classroom teachers. Materials are available on the IPC's website in the *Resources/Educational Materials* section.

The three guides were updated late in 2007 and early 2008. Included among the changes is a new lesson for high school students, *Make an Informed Online Choice*, on the potential implications of posting sensitive personal information on social networking sites.

Since the IPC's school program was launched in 1999-2000, more than 50,000 copies of the guides have been distributed.

IPC Publications

The IPC released 18 publications or videos on access and privacy topics in 2007. These included 14 new publications, updated versions of two key IPC publications, and two videos.

This year saw the release of a landmark policy paper on biometric encryption, entitled *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy*. The IPC also released two popular tip sheets, *How to Protect Your Privacy on Facebook* and *Reference Check: Is Your Boss Watching? Privacy and Your Facebook Profile*.

Two important sets of guidelines were also released: *Privacy Guidelines for Municipalities Regulating Businesses Dealing in Second-hand Goods* and an updated version of *Guidelines for the Use of Video Surveillance Cameras in Public Places*.

The IPC publications issued in 2007 were, in chronological order:

Title
• *If you wanted to know ... What is involved if you are asked to provide a Police Background Check?*
• *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy*
• *How to Avoid Abandoned Records: Guidelines on the Treatment of Personal Health Information, In the Event of a Change in Practice*
• *Checklist for Health Information Custodians in the Event of a Planned or Unforeseen Change in Practice*
• *How to Protect your Privacy on Facebook*
• *Encrypting Personal Health Information on Mobile Devices*
• The Commissioner's 2006 Annual Report
• *Safeguarding Privacy in a Mobile Workplace*
• *Wireless Communication Technologies: Video Surveillance Systems*
• *Privacy and Boards of Directors: What You Don't Know* **Can** *Hurt You* – **Updated**
• *Wireless Communication Technologies: Safeguarding Privacy & Security*
• *Privacy Guidelines for Municipalities Regulating Businesses Dealing in Second-hand Goods*
• *Guidelines for the Use of Video Surveillance Cameras in Public Places* – **Updated**
• *In Her Own Words – A compilation video of some of the Commissioner's recent TV interviews on key topics*
• *Privacy by Design 'Build it in' – A Crucial Design Principle* (video)
• *20/20 Access & Privacy Excellence – 20 Years in the Making*
• *The winter 2007 edition of the electronic newsletter, IPC Perspectives*
• *Reference Check: Is Your Boss Watching? Privacy and Your Facebook Profile*

The IPC distributed a total of 483,429 publications in 2007.

All IPC publications are available on our website at www.ipc.on.ca or by calling the Communications Department at 416-326-3333 or 1-800-387-0073.

Speeches and Presentations

The IPC has an aggressive public speaking program aimed at building awareness of privacy and access issues among government officials, CEOs and senior executives, academics, health-care decision-makers, technology-sector leaders, lawyers, privacy professionals and students.

Commissioner Cavoukian herself gave over 30 keynote presentations at major conferences and other events in 2007. These included:

- The inaugural lecture of the University of Toronto's new interdisciplinary Identity, Privacy and Security Initiative (IPSI). This initiative (www.ipsi.utoronto.ca) links two new graduate concentrations in privacy and security, offered

through the Faculty of Applied Science and Engineering and the Faculty of Information Studies. The Commissioner chairs the iPSI advisory council.

- Speeches at the international health privacy conference sponsored by the IPC and at the annual International Privacy and Data Protection Commissioners' Conference in Montreal;
- A presentation to the CBC Editorial Board, at the CBC's invitation, in which the Commissioner outlined key issues in access and privacy today and what is on the horizon;
- Presentations to the Harvard Privacy Symposium, the Emerging Leaders Forum, the annual Ontario Bar Association Privacy Summit, the International Association of Privacy Professionals, the International Association of Business Communicators, the e-Health Privacy and Security Conference, an Ontario Deputy Ministers' Council Meeting, the Ontario Hospital Association's annual conference, Havergal College, Public Safety Canada's Biometrics Working Group, the Ministry of Government Services Access and Privacy conference, and many others.

Other staff are also active in the IPC's public speaking program. This past year, for example, the IPC's two Assistant Commissioners – Ken Anderson and Brian Beamish – and other senior staff made presentations to audiences ranging from government officials and universities to health-care organizations, the police, and the private sector.

Presentations are also delivered each year as part of the IPC's *Reaching Out to Ontario* program. For example, while in St. Catharines for the IPC's *Niagara Region Educational Initiative* in late 2007, IPC staff participated in a videoconference session about Ontario's *Personal Health Information Protection Act* with a group of Ontario hospitals. The session was also shown as a webcast.

Media Relations

The IPC has a proactive media relations program to help raise the media's – and thus the public's – awareness of access and privacy issues.

The program includes presentations to editorial boards and newsroom staff on the role of the IPC and on access and privacy issues. In 2007, the Commissioner presented to the CBC's Editorial Board, while other presentations were made to members of the news teams at the St. Catharines Standard and the Niagara Falls Review and to journalism, electronic media and other students at Mohawk, Niagara, Centennial and Humber Colleges. The Commissioner gave 97 interviews to media organizations from across Canada and around the world.

IPC staff take media inquiries relating to freedom of information, protection of privacy, and the *Personal Health Information Protection Act*. This year, the IPC assisted more than 180 journalists who requested interviews or background information or who had general inquiries about access and privacy, including how to file freedom of information requests.

The Commissioner also issued 18 news releases in 2007.

IPC Website

The IPC has a rich and ever-expanding website at www.ipc.on.ca. It provides access to IPC publications and orders, links to copies of the three Ontario *Acts* governing access and privacy, answers to frequently asked questions, educational material, news releases, selected speeches, forms, and much more.

The most downloaded items in 2007 included a tip sheet, *How to Protect Your Privacy on Facebook*, and *HO-004*, the Commissioner's order dealing with the need to encrypt personal health information that is stored on an electronic device for work at home or on the road. The order followed an IPC investigation into the theft from a doctor's vehicle of a laptop computer containing the personal health information of 2,900 patients at Toronto's Hospital for Sick Children.

Other frequently downloaded publications included the Commissioner's 2006 Annual Report, released in May 2007, the *Breach Notification Assessment Tool* and a fact sheet, *Encrypting Personal Health Information on Mobile Devices*.

Part of the IPC's mandate under the *Acts* is to offer comment on the privacy and access implications of proposed government legislation or programs and on the existing or proposed information practices of health information custodians.

In 2007, the IPC commented on the following:

Provincial Consultations

Ministry of Community Safety and Correctional Services:
- Bill 28, Implementation of the Mandatory Blood Testing Act, 2006

Ministry of Community and Social Services:
- Bill 12, Access to Adoption Records Act (Vital Statistics Statute Law Amendment), 2007
- Implementation of Good Parents Pay website
- Bill 165 – Provincial Advocate for Children and Youth Act, 2007 (Ministry of Community and Social Services and with the Ministry of Children and Youth Services)

Ministry of Government Services:
- ServiceOntario Driver and Vehicle Services
- Bill 184, Endangered Species Act, 2007 (related to consequential amendments to *FIPPA*)
- Bill 152, Implementation of amendments to the Change of Name Act

Ministry of Labour
- Bill 69, Implementation of the Regulatory Modernization Act, 2007

Municipal Consultations

Ottawa Police Services:
- Community Safety Letter Program

City of Ottawa, City of Oshawa and Ontario Association of Chiefs of Police:
- Regulation of businesses dealing in second-hand goods

Health Information Custodian Consultations

Ministry of Health and Long-Term Care
- Review of Smart Systems for Health Agency information practices

The IPC also worked with numerous non-government health information custodians on matters related to the *Personal Health Information Protection Act, 2004 (PHIPA)* this year. These included the health professions associations and regulating colleges, prescribed registries and entities under *PHIPA*, individual hospitals and others.

Submissions and Special Reports

A letter from Commissioner Ann Cavoukian to the Honourable Stockwell Day, Minister of Public Safety, regarding "Lawful Access" and Customer Name and Address Information.

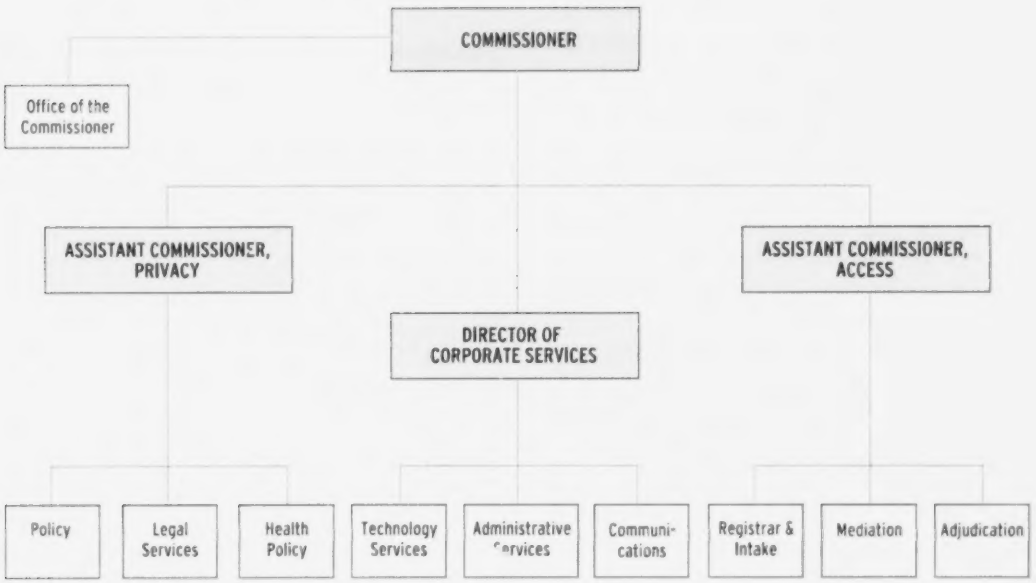
A letter from Assistant Commissioner Ken Anderson to the Honourable Donald H. Oliver, Senator, Chair of the Standing Senate Committee on Legal and Constitutional Affairs, regarding Bill C-31 (An Act to amend the Canada Elections Act and the Public Service Employment Act).

A letter and submissions from Commissioner Ann Cavoukian to the Toronto Police Services Board regarding the Review of a Proposed Policy Regarding the "Destruction of Adult Fingerprints, Photographs and Records of Disposition."

A letter from Assistant Commissioner Ken Anderson to the Honourable Lawrence Cannon, Minister of Transport, Infrastructure and Communities, regarding the Proposed Federal Identity Screening Regulations and the Interrelated Passenger Protect Program.

All four of these submissions can be found in the *Resources* section of the IPC's website, www.ipc.on.ca.

ORGANIZATIONAL CHART



FINANCIAL STATEMENT

	2007-2008 Estimates	2006-2007 Estimates	2006-2007 Actual
	$	$	$
Salaries and wages	8,773,000	8,239,000	7,995,877
Employee benefits	1,886,200	1,771,500	1,440,032
Transportation and Communications	323,700	323,700	293,308
Services	1,523,800	1,523,800	1,732,345
Supplies and Equipment	274,800	274,800	535,833
Total	**12,781,500**	**12,132,800**	**11,997,394**

Note: The IPC's fiscal year begins April 1 and ends March 31.

The financial administration of the IPC is audited on an annual basis by the Office of the Auditor General of Ontario.

Public Sector Salary Disclosure

As required by the Public Sector Salary Disclosure Act, 1996, the following chart shows which IPC employees received more than $100,000 in salary and benefits for the calendar year ending December 31, 2007.

Name	Position	Earnings	Taxable Benefits
		$	$
Cavoukian, Ann	Commissioner	193,773.33	352.17
Anderson, Ken	Assistant Commissioner (Privacy)	203,110.79	338.49
Beamish, Brian	Assistant Commissioner (Access)	203,110.79	338.49
Binstock, Robert	Registrar	121,976.46	202.73
Carter, Fred	Senior Policy & Technology Advisor	107,713.24	179.35
Challis, William	General Counsel	199,369.07	338.49
Chibba, Michelle	Director, Policy	120,499.90	201.82
Cropley, Laurel	Adjudicator	101,851.28	172.97
DeVries, Frank	Adjudicator	102,271.53	173.10
Faughnan, Steven	Adjudicator	116,379.11	191.37
Geisberger, Janet	Director, Corporate Services	126,181.62	213.60
Goldstein, Judith	Legal Counsel	179,666.48	310.86
Goodis, David	Legal Counsel	179,666.48	310.86
Grant, Debra	Senior Health Privacy Specialist	112,958.53	181.47
Hale, Donald	Team Leader, Adjudication	130,628.67	207.28
Higgins, John	Manager, Adjudication	183,102.92	310.86
Jiwan, Mumtaz	Team Leader, Mediation (Provincial)	104,057.11	164.72
Khandor, Ramesh	Legal Counsel	106,693.37	168.49
Liang, Sherry	Legal Counsel	110,123.95	210.63
McCammon, Stephen	Legal Counsel	130,300.50	234.34
Morrow, Bernard	Adjudicator	116,379.11	191.37
O'Donoghue, Mary	Manager, Legal Services	195,627.35	338.49
Pascoe, Irena	Team Leader, Mediation (Municipal)	100,464.72	164.72
Senoff, Shirley	Legal Counsel	128,310.76	230.74
Smith Douglas, Diane	Adjudicator	119,024.13	112.00
Swaigen, John	Legal Counsel	183,102.92	310.86
Wong, Mona	Manager of Mediation	121,874.00	202.73

DESIGN: nectar design + communications www.nectardesign.ca PRINTED IN CANADA: Clockwork Productions Inc.

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8

Tel: 416 326 3333
Fax: 416 325 9195

1 800 387 0073
TTY: 416 325 7539

www.ipc.on.ca